Data Communications and Networking Fourth Edition

Forouzan

Capítulo 20

Camada de Rede: Protocolo de Internet

20-1 INTERNETWORKING

Esta seção trata do conceito de internetworking, isto é, a conexão entre redes.

Tópicos discutidos nessa seção:

Necessidade da camada de rede
Internet como uma rede de datagramas
Internet como uma rede sem conexão

Figura 20.1 *Enlaces entre dois hosts*

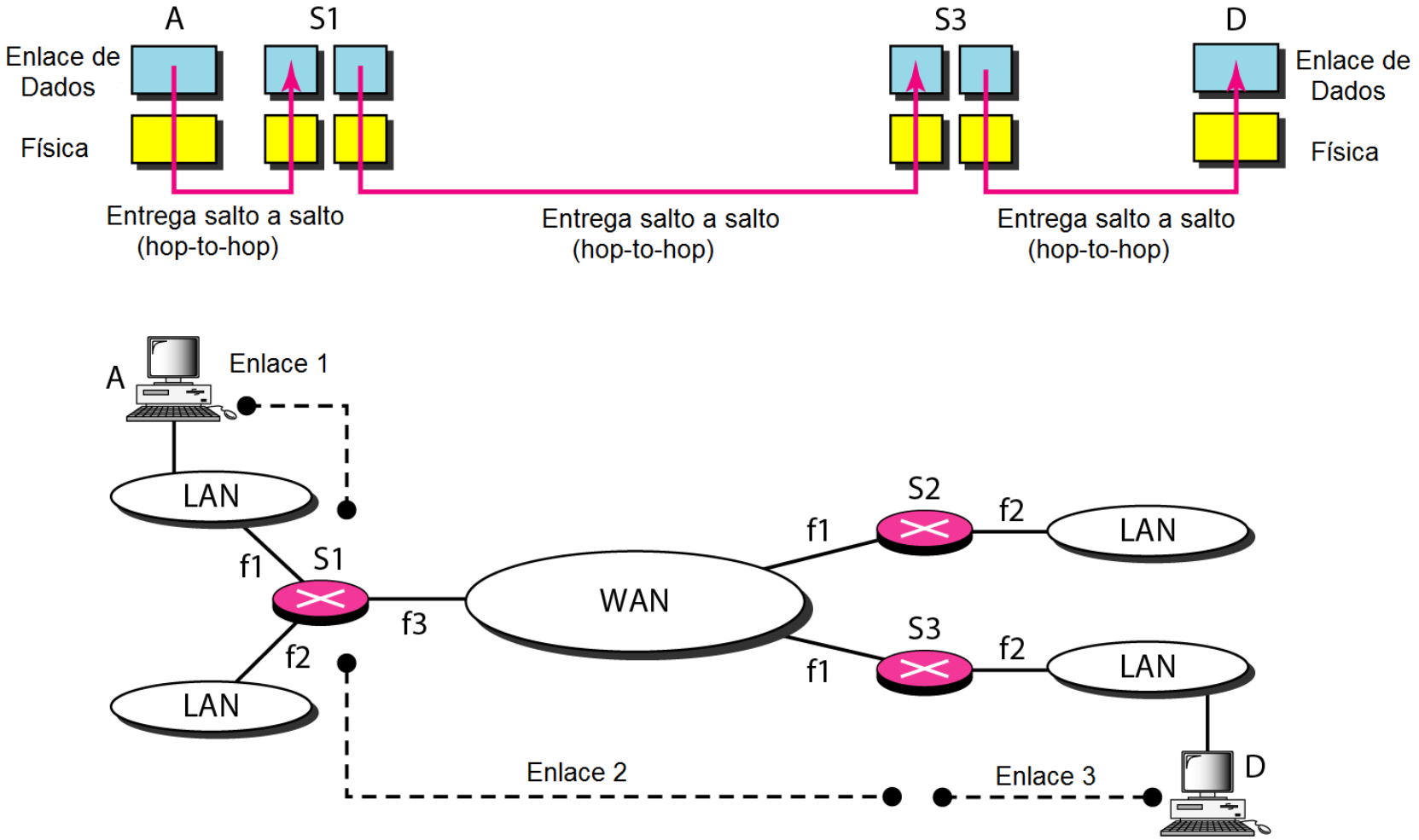


Figura 20.2 *A Camada de Rede em uma inter-rede*

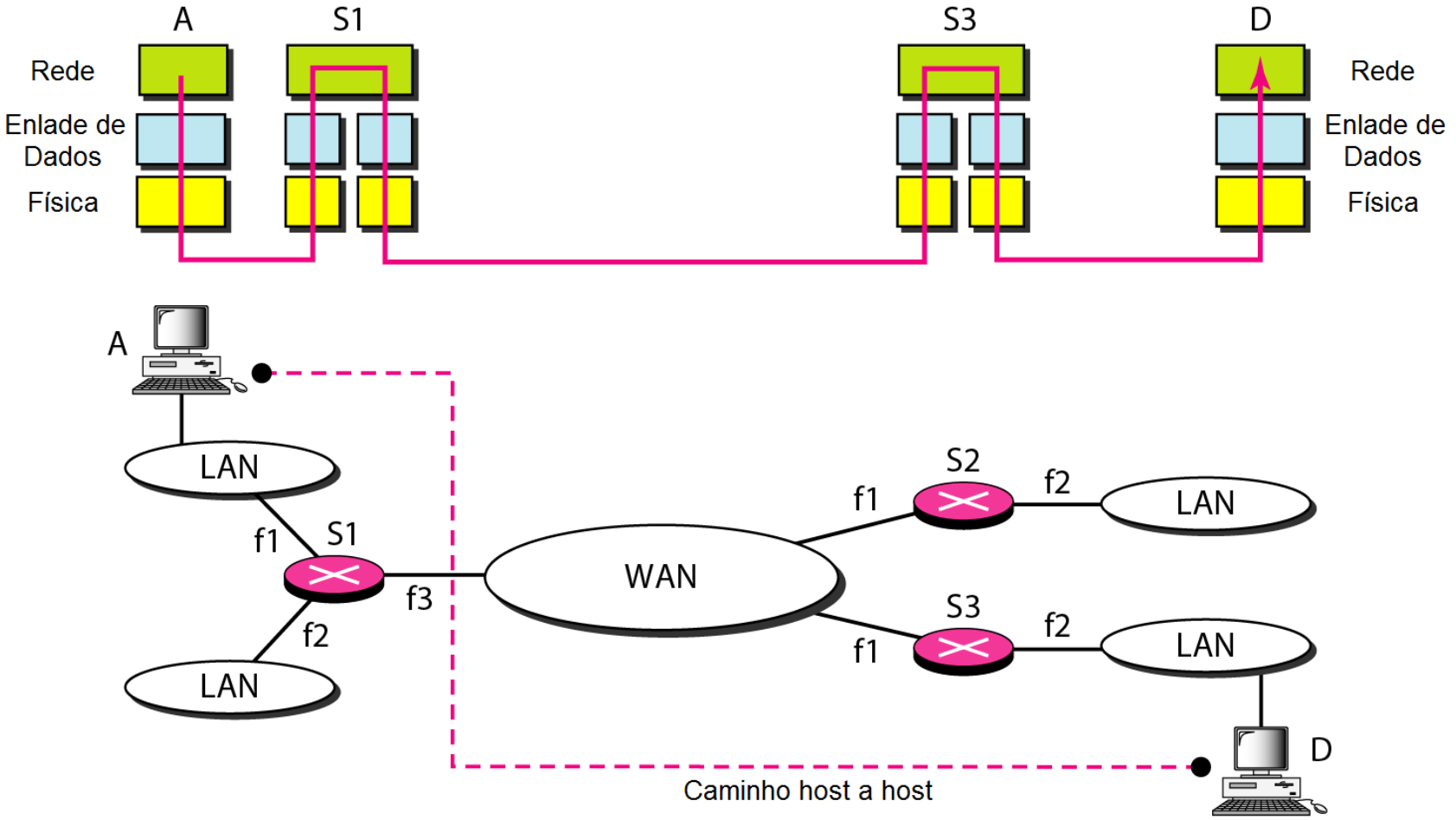


Figura 20.3 *Camada de Rede na origem e no destino*

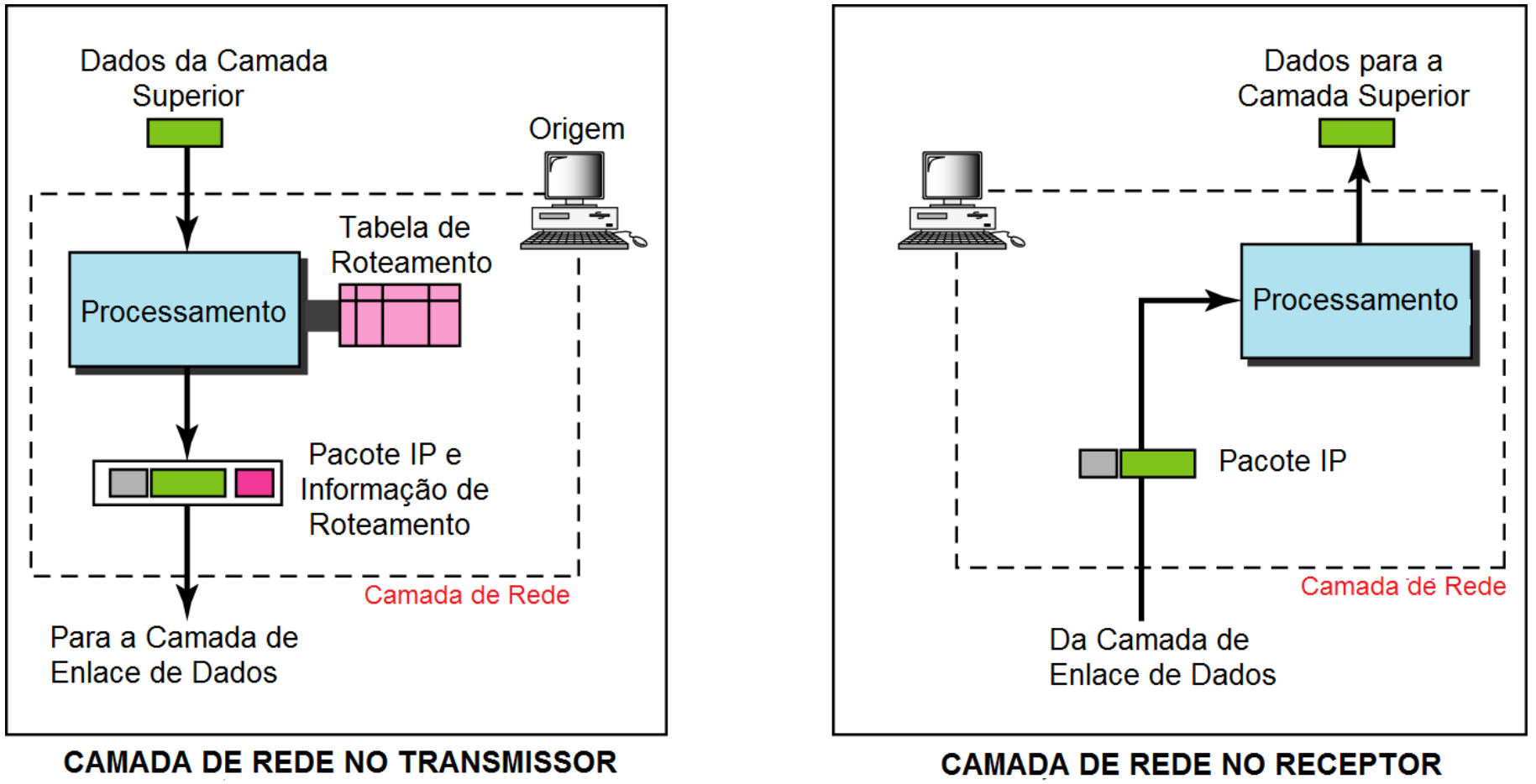
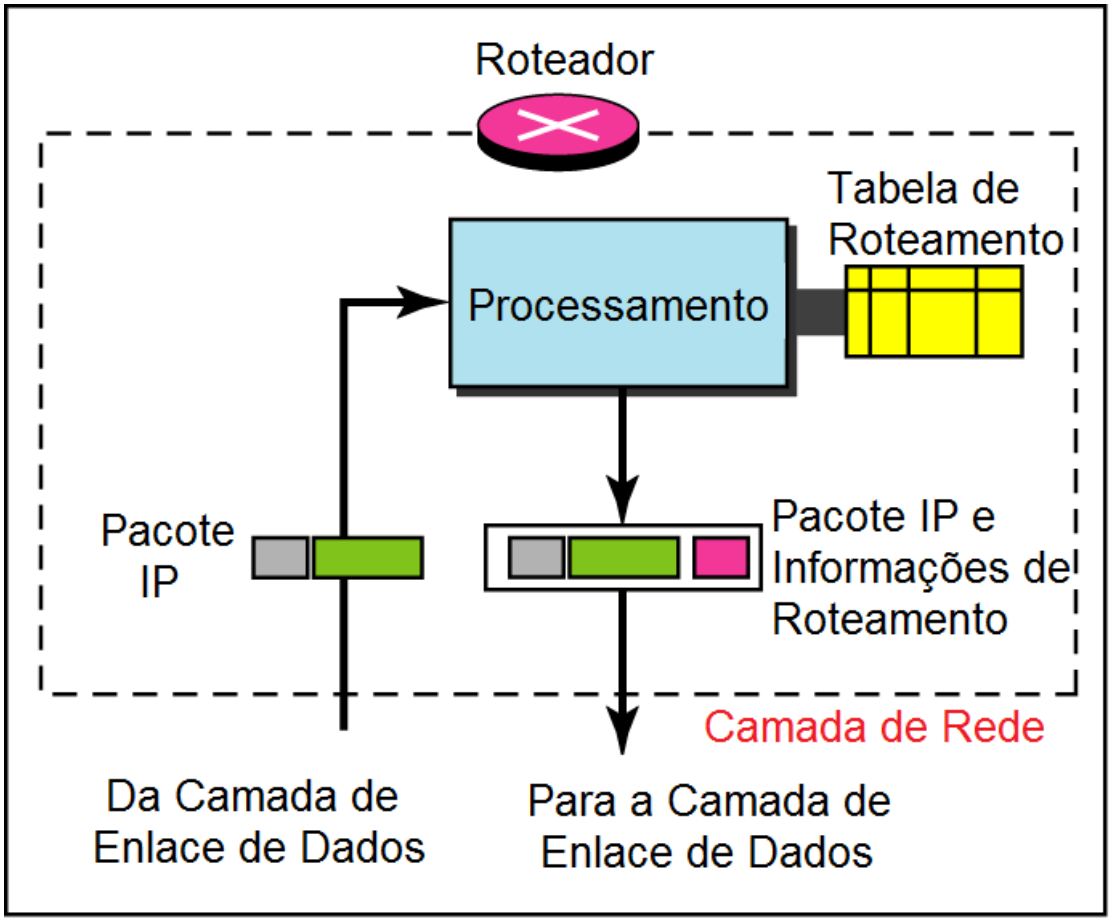


Figura 20.3 *Camada de Rede no roteador*



CAMADA DE REDE EM UM ROTEADOR

Nota

A comutação na camada de rede na Internet utiliza a abordagem de datagramas para comutação de pacotes.

Nota

A comunicação na camada de rede na Internet é sem conexão.

20-2 IPv4

O Protocolo de Internet versão 4 (IPv4) é usado na entrega de dados pelo protocolo TCP / IP.

Tópicos discutidos nessa seção:

Datagrama
Fragmentação
Checksum (Soma de Verificação)
Opções

Figura 20.4 *Posicionamento do IPv4 na Pilha de Protocolos TCP/IP*

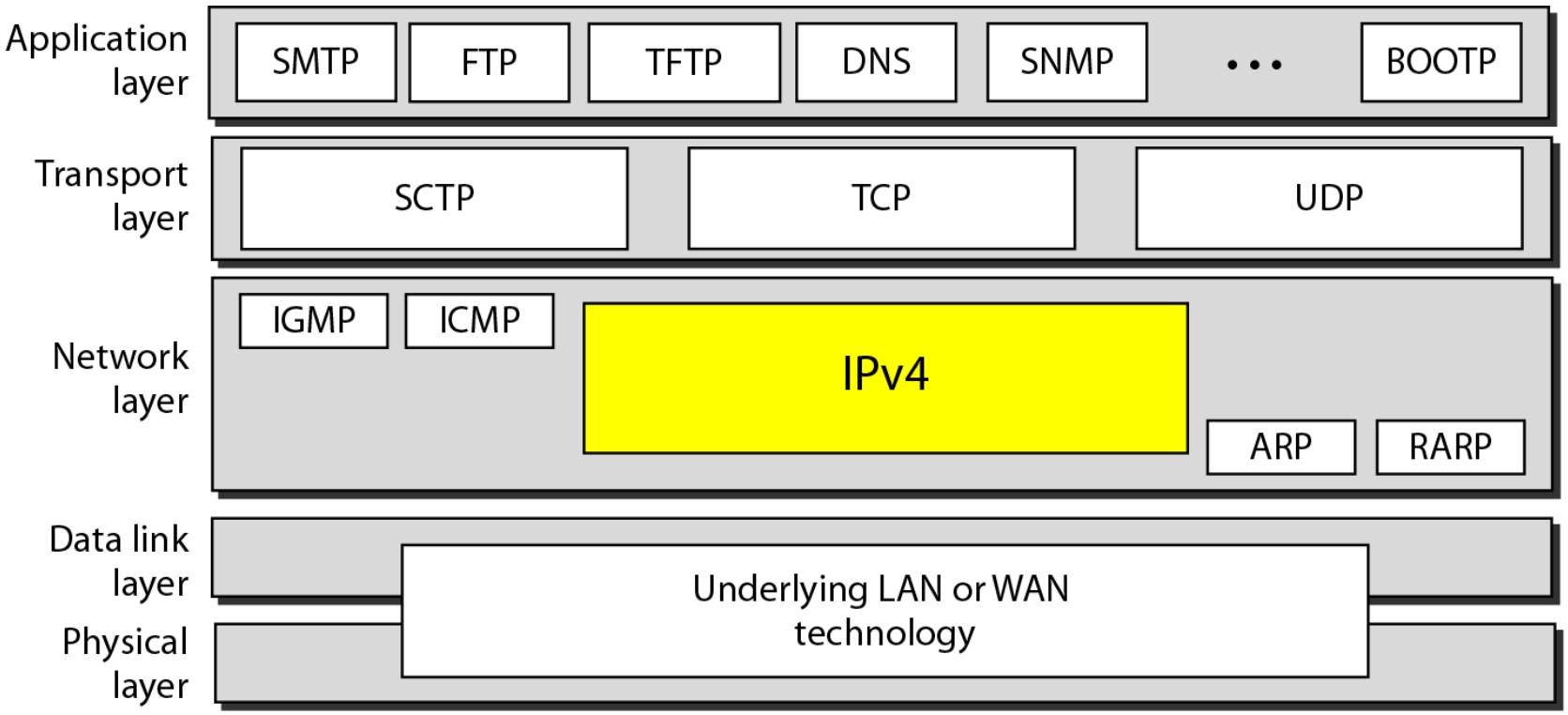
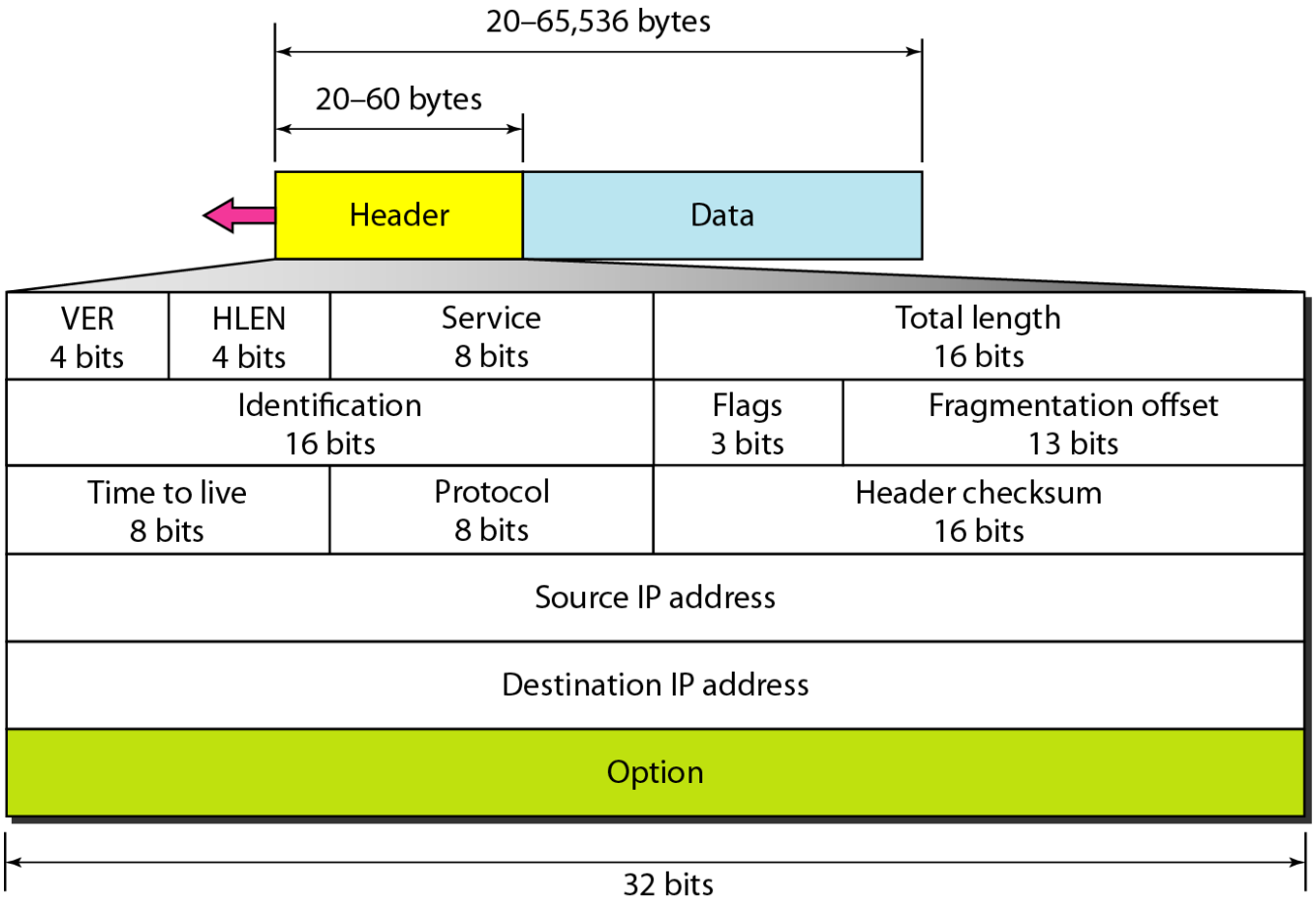


Figura 20.5 *Formato do datagrama IPv4*



Campos do Datagrama IPv4

Campo	Significado
VER	Versão do protocolo IP (versão 4)
HLEN	Tamanho do cabeçalho. Multiplica-se o valor desse campo por 4 (em bytes)
Service	Tipo de Serviço (Serviços Diferenciados)
Total Length	Tamanho total do datagrama (cabeçalho + dados) em bytes – max = 65.535 bytes
TTL	Tempo de vida, em nº de saltos
Protocol	Protocolo de camada superior (ex: TCP)

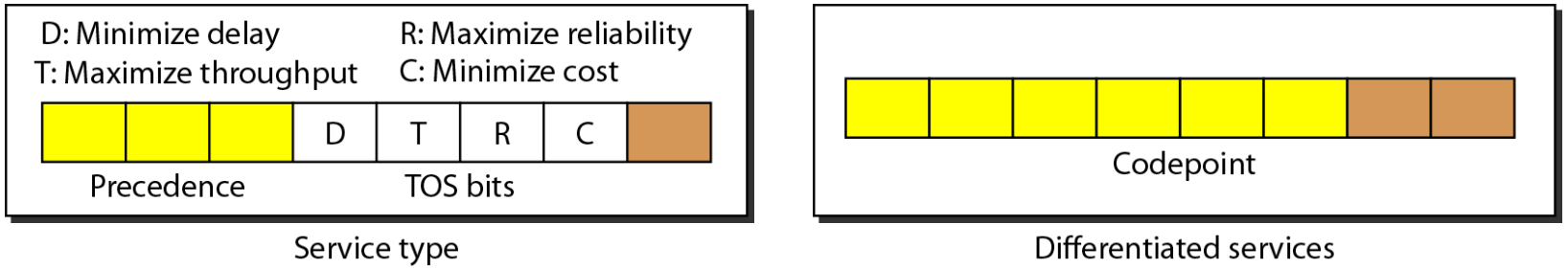
Campos do Datagrama IPv4 (continuação)

Campo	Significado
Identification	Identificação do datagrama, usado na fragmentação
Flags (3 bits)	1º bit é reservado; 2º bit: 1=não fragmentar, 0=fragmentar; 3º bit: 1=mais fragmentos, 0=último fragmento
Fragmentation Offset	Posição relativa de um fragmento no datagrama (em unidades de 8 bytes)
Header Checksum	Soma de verificação do cabeçalho (verificação de erros)

Campos do Datagrama IPv4 (continuação)

Campo	Significado
Source IP	Endereço IP de origem
Destination IP	Endereço IP de destino
Option	Campos não obrigatórios no Datagrama IP. Usados para testes e depuração da rede

Figura 20.6 *Tipo de serviço ou Serviços Diferenciados*



Nota

O subcampo precedência é parte da versão 4, mas nunca foi usado.

Tabela 20.1 *Tipos de Serviço*

Bits TOS	Descrição
0000	Normal (default)
0001	Minimizar Custo
0010	Maximizar confiabilidade
0100	Maximizar Vazão
1000	Minimizar Atraso

Tabela 20.2 *Tipos de serviço Default*

Protocolo	Bits ToS	Descrição
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimizar custo
IGP	0010	Maximizar confiabilidade
SNMP	0010	Maximizar confiabilidade
TELNET	1000	Minimizar atraso
FTP (dados)	0100	Maximizar vazão
FTP (controle)	1000	Minimizar atraso
SMTP (comando)	1000	Minimizar atraso
SMTP (dados)	0100	Maximizar vazão
DNS (consulta UDP)	1000	Minimizar atraso
DNS (consulta TCP)	0000	Normal
DNS (zona)	0100	Maximizar vazão

Tabela 20.3 *Valores do codepoints*

Category	*Codepoint*	*Assigning Authority*
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or experimental

Nota

O campo comprimento total define o comprimento total do datagrama, incluindo cabeçalho.

Figura 20.7 ***Encapsulamento de um datagrama pequeno em um quadro Ethernet***

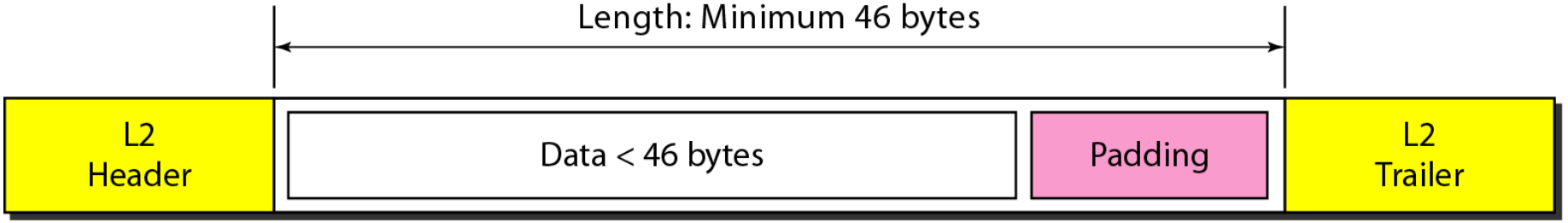


Figura 20.8 *Campo Protocolo e dados encapsulados*

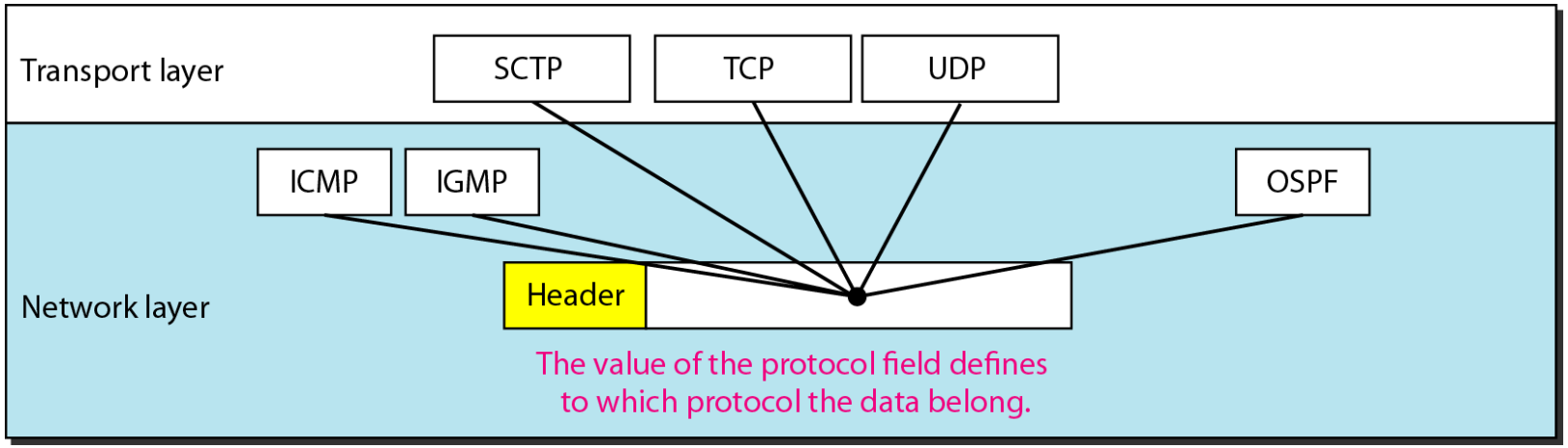


Tabela 20.4 *Valores de Protocolo*

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Exemplo 20.1

Um IPv4 pacote chegou com os primeiros 8 bits do cabeçalho, conforme mostra abaixo

01000010

O receptor descartou o pacote. Por que?

Solução

Existe um erro neste pacote. Os 4 bits mais à esquerda (0100) mosram a versão, que está correto. Os próximos 4 bits (0010) mostam um tamanho de cabeçalho inválido (2 × 4 = 8). O nº mínimo de bytes no cabeçalho deve ser 20. The pacote foi corrompido na transmissão.

Exemplo 20.2

Em um pacote IPv4, o valor de HLEN é 1000 em binário. Quantos bytes de opções estão sendo realizadas por esse pacote?

Solução

O valor de HLEN é 8, o que siginifica que o nº total de bytes do cabeçalho é 8 × 4, ou 32 bytes. Os primeiros 20 bytes são usados pelo cabeçalho padrão, os próximos 12 bytes são as opções.

Exemplo 20.3

Em um pacote IPv4 pacote, o valor de HLEN é 5, e o valor do campo tamanho total é 0x0028. Quantos bytes de dados são carregados por este pacote?

Solução

O valor de HLEN é 5, o que significa que o nº total de bytes no cabeçalho é 5 × 4, ou 20 bytes (sem opções). O tamanho total é 40 bytes, o que significa que o pacote está carregando 20 bytes de dados (40 − 20).

Exemplo 20.4

Um pacote IPv4 chegou com os primeiros digitos em hexadecimal abaixo.

*0x450000280001000001**02** . . .*

Quantos hops este pacote pode viajar antes de ser descartado? Os dados pertencem a qualquer protocolo de camada superior?

Solução

Para encontrar o campo TTL (tempo de vida), desprezamos os primeiros 8 bytes. O campo TTL é o nono byte, que é igual a 01. Isto siginifica que o pacote pode viajar para apenas 1 hop. O campo protocolo é o próximo byte (02), o que significa que protocolo de camada superior é IGMP.

Figura 20.9 *MTU – Unidade Maxima de Transferência*

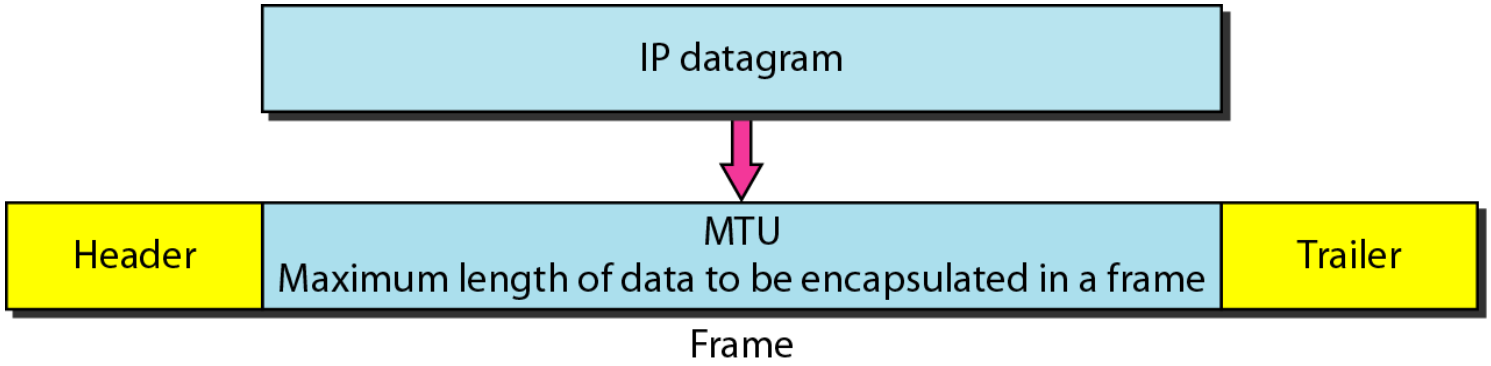


Tabela 20.5 ***MTUs em bytes para algumas redes***

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Figura 20.10 *Necessidade da Fragmentação*

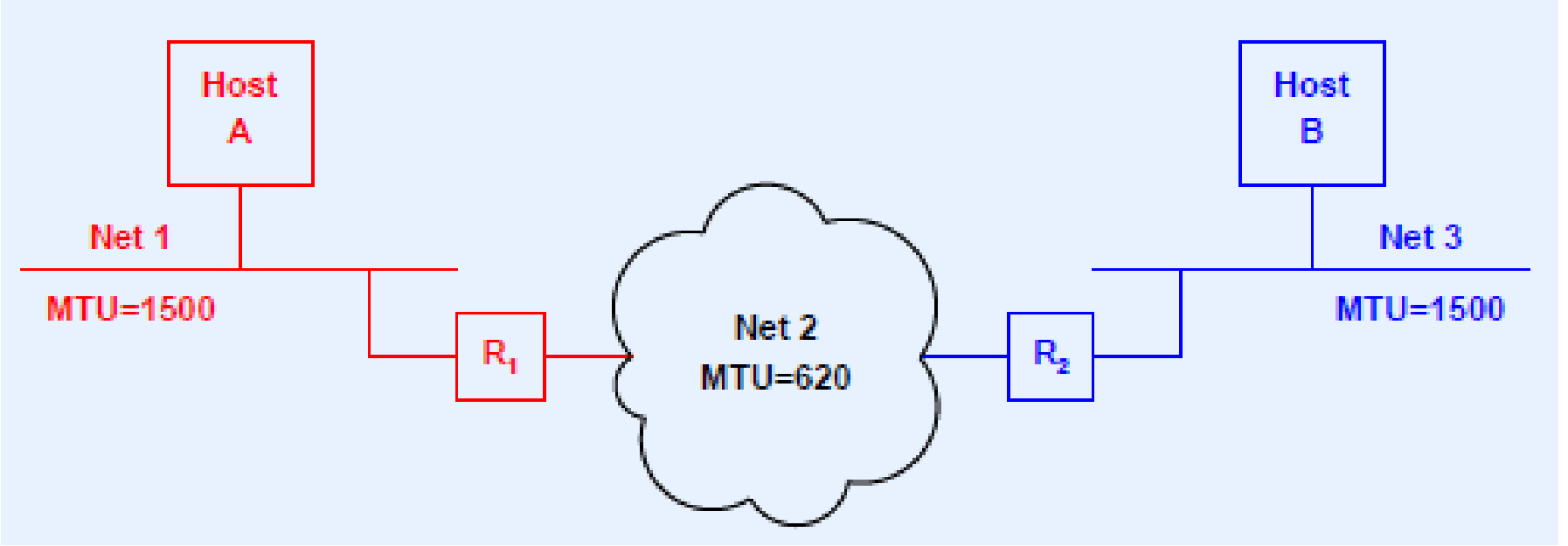
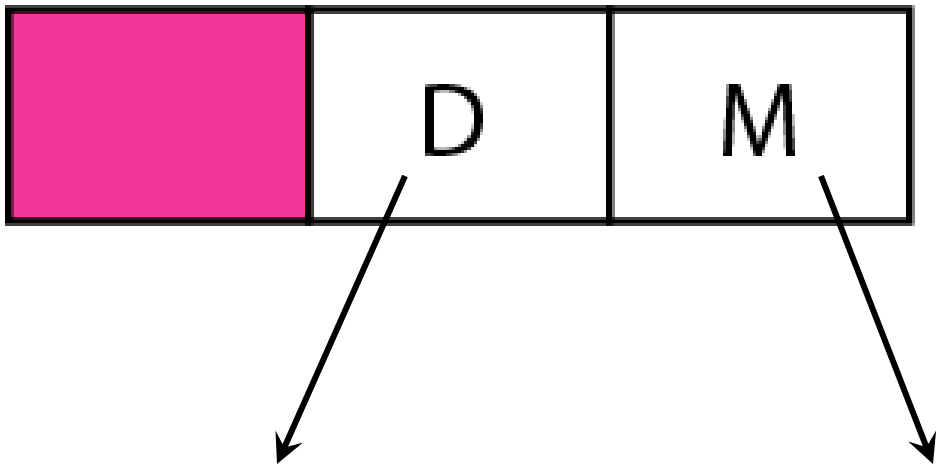


Figura 20.11 *Flags usados na fragmentação*



D – não fragmentar

se for 1, o host não deve fragmentar o datagrama

se for 0, o host deve fragmentar o datagrama

M – mais fragmentos

se for 1, existem mais fragmentos

se for 0, é o último fragmento do datagrama

Figura 20.12 *Exemplo de fragmentação*

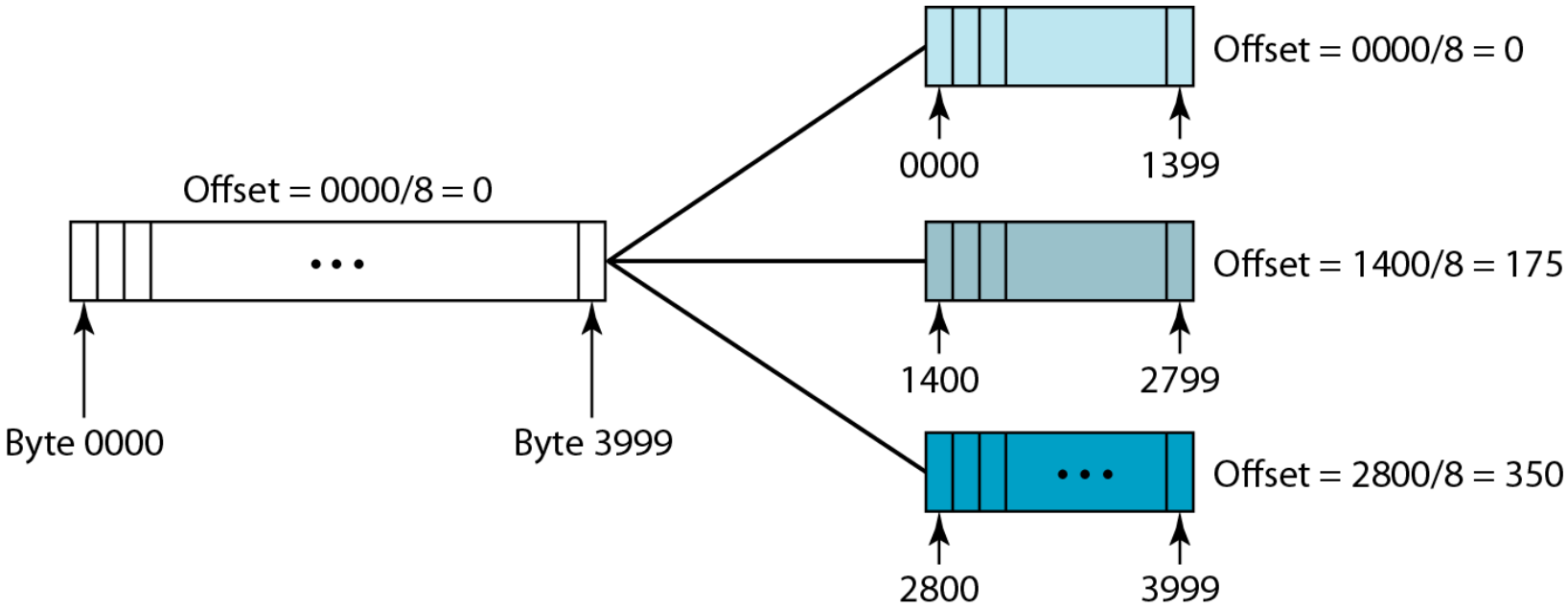
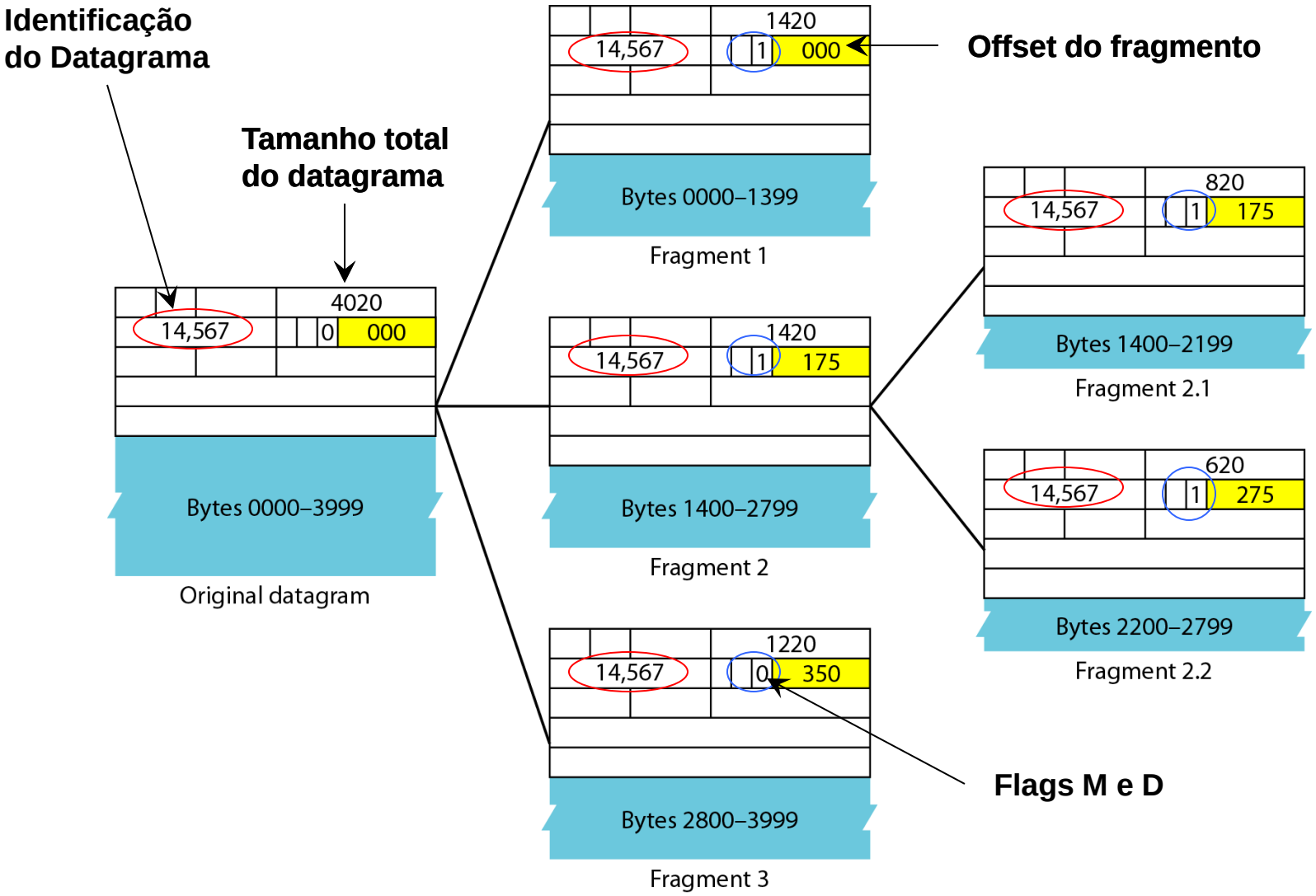


Figura 20.13 *Exemplo detalhado de fragmentação*



Exemplo 20.5

Um pacote chegou com um valor do bit M igual a 0. Qual o tipo de fragmento? Primeiro, último ou intermediário? Este pacote foi fragmentado? Como obter essa informação?

Solução

Se o bit M é 0, significa que não há mais fragmentos, ou seja, o fragmento é o último. Contudo, não podemos dizer se o pacote original foi fragmentado ou não. Um pacote não fragmentado é considerado o útimo fragmento.

Exemplo 20.6

Um pacote chegou com o valor do M bit igual a 1. Qual o tipo de fragmento? Primeiro, último ou intermediário? Este pacote foi fragmentado? Como obter essa informação?

Solução

Se o bit M é 1, significa que existe pelo menos mais 1 fragmento. Este fragmento pode ser o primeiro ou 1 fragmento intermediário, mas não é o último. Não sabemos se é o o primeiro ou 1 fragmento intermediário; é necessário mais informações (o valor do offset do fragmentação).

Exemplo 20.7

Um pacote chegou com o valor do bit M é igual a 1 e o valor do offset do fragmento é igual a 0. Qual o tipo de fragmento? Primeiro, último ou intermediário?

Solução

Como o valor do bit M é igual a 1, ele pode ser o primeiro fragmento ou um fragmento intermediário. Como o valor do offset do fragmento é 0, ele é o primeiro fragmento.

Exemplo 20.8

Um pacote chegou com o valor do offset igual a 100. Qual é o nº do primeiro byte? É possível obter o nº do último byte?

Solução

Para encontrar o nº do primeiro byte, multiplica-se o valor do offset por 8. Isto significa que o nº do primeiro byte é 800. Não há como determinar o nº do último byte, a não ser que seja conhecido o tamanho do datagrama.

Exemplo 20.9

Um pacote chegou com o valor do offset igual a 100, o valor de HLEN é 5, e o valor do campo tamanho total é 100. Quais os números do primeiro byte e do último byte?

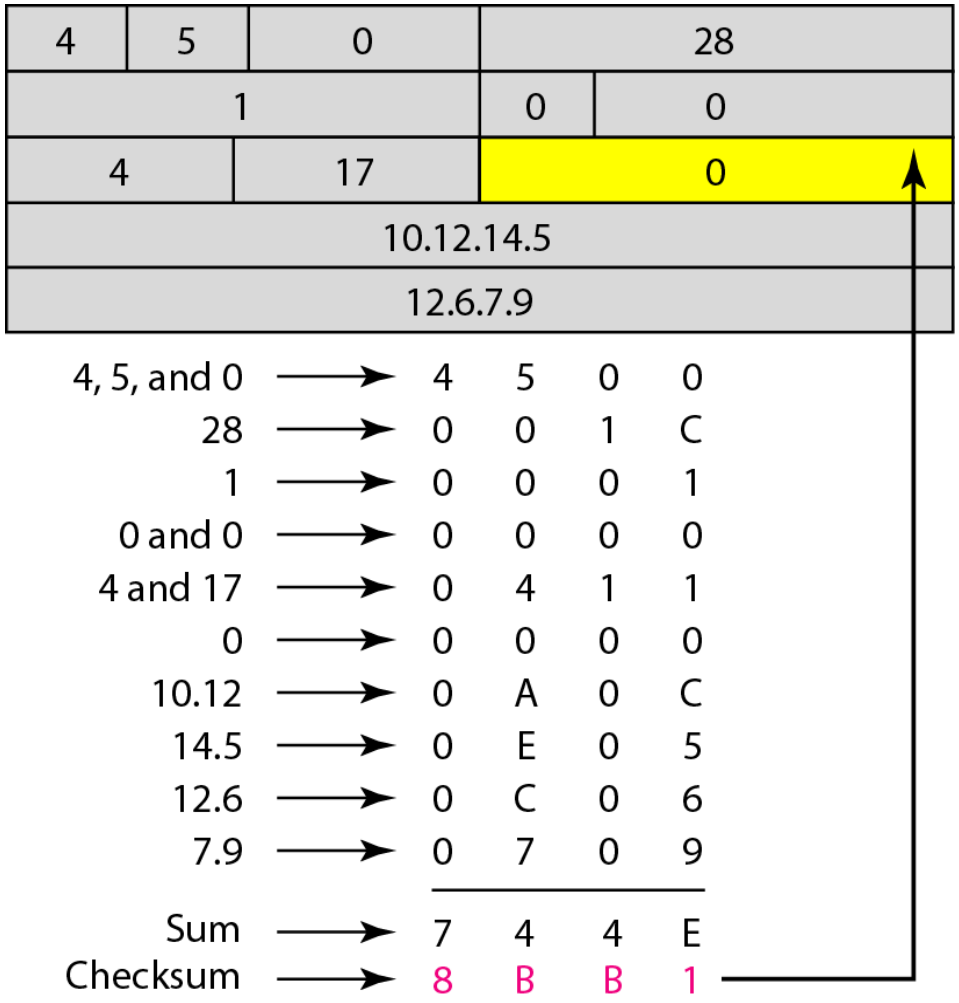
Solução

O número do primeiro byte é 100 × 8 = 800. O tamanho total é 100 bytes, e o tamanho do cabeçalho é 20 bytes (5 × 4), o que significa que existem 80 bytes no datagrama. Se o número do primeiro byte é 800, o número do último byte deve ser 879.

Exemplo 20.10

A Figura 20.13 mostra um exemplo de cálculo do checksum de um cabeçalho IPv4, sem opções. O cabeçalho é dividido em seções de 16 bits. Todas as seções são acrescentadas e a soma é complementada. O resultado é inserido no campo checksum.

Figura 20.14 *Exemplo de cálculo do checksum no IPv4*



20-3 O Datagrama IPv6

A protocolo de camada de Rede no modelo TCP/IP atualmente é o IPv4. O IPv4 foi projetado considerando o cenário de comunicação de dados na década de 1970. Com o crescimento rápido da Internet, foram detectadas várias deficiências no IPv4.

Tópicos discutidos nessa seção:

Vantagens do IPv6
Formato do Pacote
Cabeçalhos de Extenssão

Vantagens do IPv6

- **Maior espaço de endereços.** Um endereço IPv6 tem 128 bits de comprimento, conforme já discutido no Capítulo 19. Comparado com um endereço de 32 bits do IPv4, este representa um aumento enorme (2^{96}) no espaço de endereços.
- **Formato mais adequado do cabeçalho.** O IPv6 usa um novo formato de cabeçalho, no qual as opções são separadas do cabeçalho-base e inseridas, quando necessário, entre o cabeçalho-base e os dados da camada superior. Isso simplifica e acelera o processo de roteamento, pois grande parte das opções não precisam ser processadas pelos roteadores.
- **Novas opções.** O IPv6 acrescenta novas opções para possibilitar funcionalidades adicionais.
- **Espaço para expansão.** O IPv6 foi desenvolvido para permitir a extensão do protocolo, caso seja preciso suportar novas tecnologias ou aplicações.
- **Suporte para alocação de recursos.** No IPv6, o campo tipo de serviço foi eliminado, mas um mecanismo (denominado **flow label — rótulo de fluxo**) foi acrescentado para permitir que a origem solicite tratamento especial de um pacote. Esse mecanismo pode ser usado para suportar tráfego como áudio e vídeo em tempo real.
- **Melhor suporte à segurança.** As opções de criptografia e autenticação no IPv6 oferecem confidencialidade e integridade para os pacotes.

Figura 20.15 *Cabeçalhos do datagrama IPv6 e carga útil*

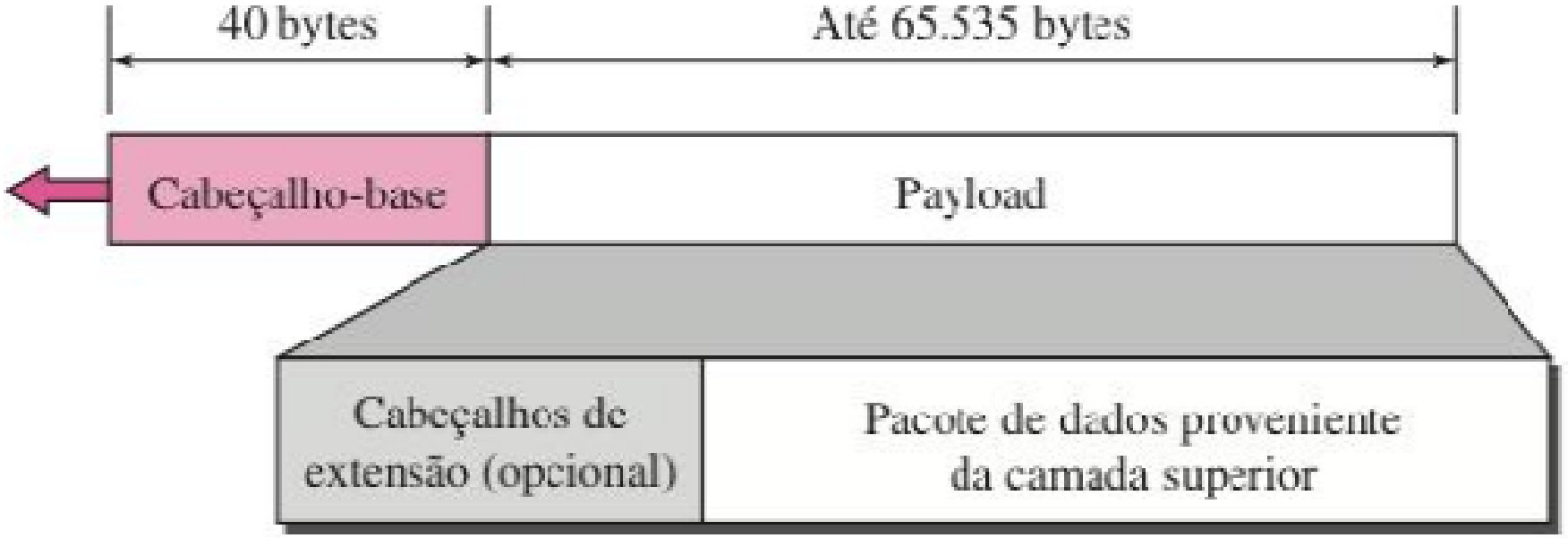


Figura 20.16 *Formato de um datagrama IPv6*

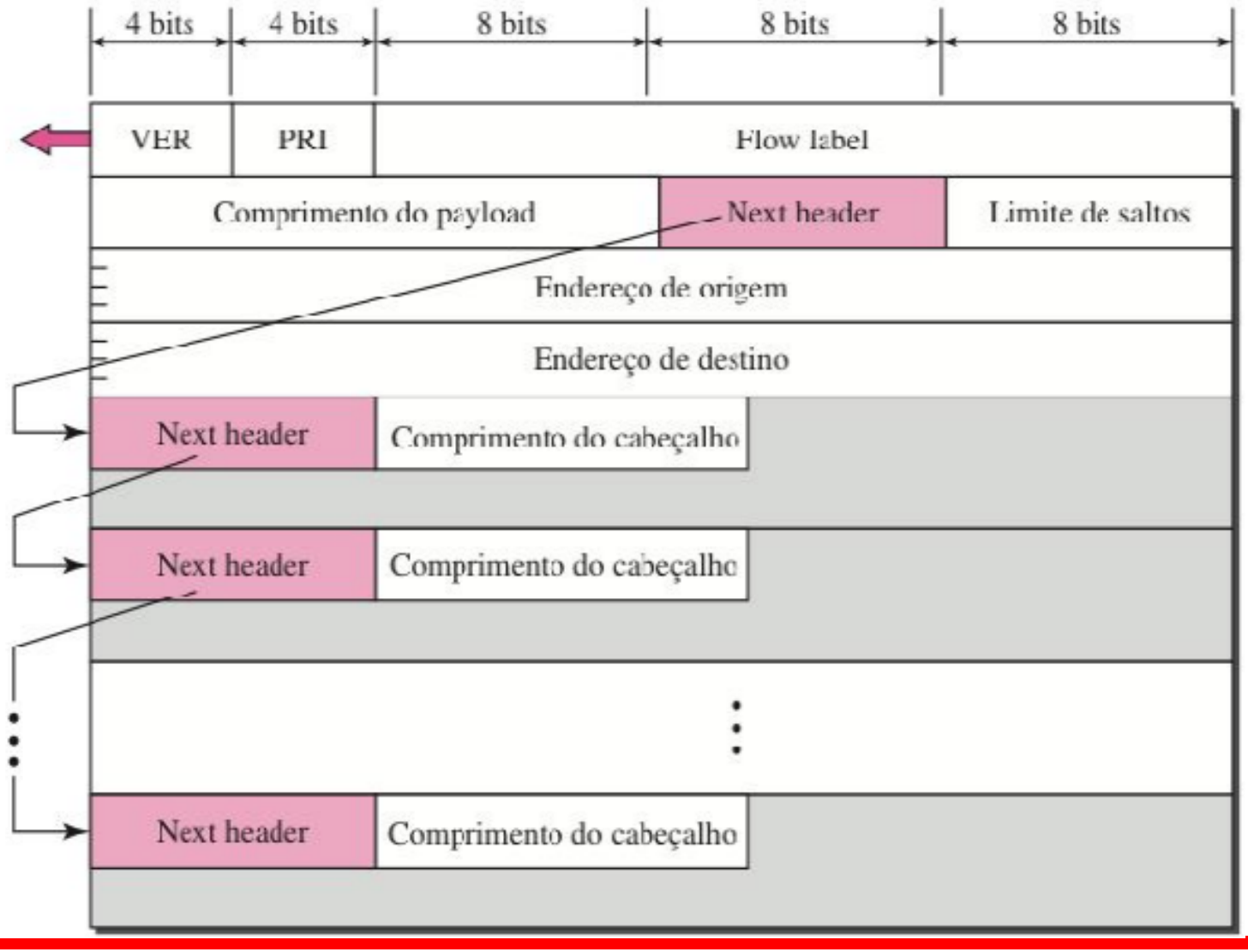


Tabela 20.6 *Códigos do campo Next Header (próximo cabeçalho) no IPv6*

Código	Próximo Cabeçalho (Next Header)
0	Opção hop-a-hop
2	ICMP
6	TCP
17	UDP
43	Roteamento na origem
44	Fragmentação
50	Carga útil criptografada
51	Autenticação
59	Null (não há próximo cabeçalho)
60	Opção de destino

Tabela 20.7 ***Prioridades para tráfego controlado por congestionamento***

Prioridade	Significado
0	Nenhum tráfego específico
1	Dados de background
2	Tráfego de dados isolado
3	Reservado
4	Tráfego de dados pesado atendido
5	Reservado
6	Tráfego Interativo
7	Tráfego de Controle

Tabela 20.8 ***Prioridades tráfego não controlado por congestionamento***

Prioridade	Significado
8	Dados com maior redundância
....	
15	Dados com menor redundância

Tabela 20.9 *Comparação dos cabeçalhos dos pacote IPv4 e IPv6*

Comparação
1. O campo de comprimento do cabeçalho é eliminado no IPv6, pois o comprimento do cabeçalho é fixo nessa versão.
2. O campo de tipo de serviço é eliminado no IPv6. Os campos de prioridade e de rótulo de fluxo, juntos, assumem a função do campo tipo de serviço.
3. O campo comprimento total é eliminado no IPv6 e substituído pelo campo de comprimento do payload.
4. Os campos de identificação, flag e offset são eliminados do cabeçalho-base no IPv6. Eles são inclusos no cabeçalho de extensão de fragmentação.
5. O campo TTL chama-se limite de saltos no IPv6.
6. O campo de protocolo é substituído pelo campo next header.
7. O checksum do cabeçalho é eliminado, pois o checksum já é calculado pelos protocolos de camada superior; portanto, ele não é necessário neste nível.
8. Os campos de opções do IPv4 são implementados como cabeçalhos de extensão no IPv6.

20-4 TRANSIÇÃO DO IPv4 PARA IPv6

Devido ao grande crescimento do nº de sistemas na Internet, a transição do IPv4 para o IPv6 não pode ocorrer repentinamente. Deve levar muito tempo para que cada sistema na Internet possa migrar do IPv4 para o IPv6. A transição deve ser feita paulatinamente para prevenir qualquer problema entre sistemas IPv4 e IPv6 systems.

Tópicos discutidos nessa seção:

Pilha Dupla
Tunelamento
Cabeçalho de Tradução

Figura 20.18 *3 estratégias de transição*

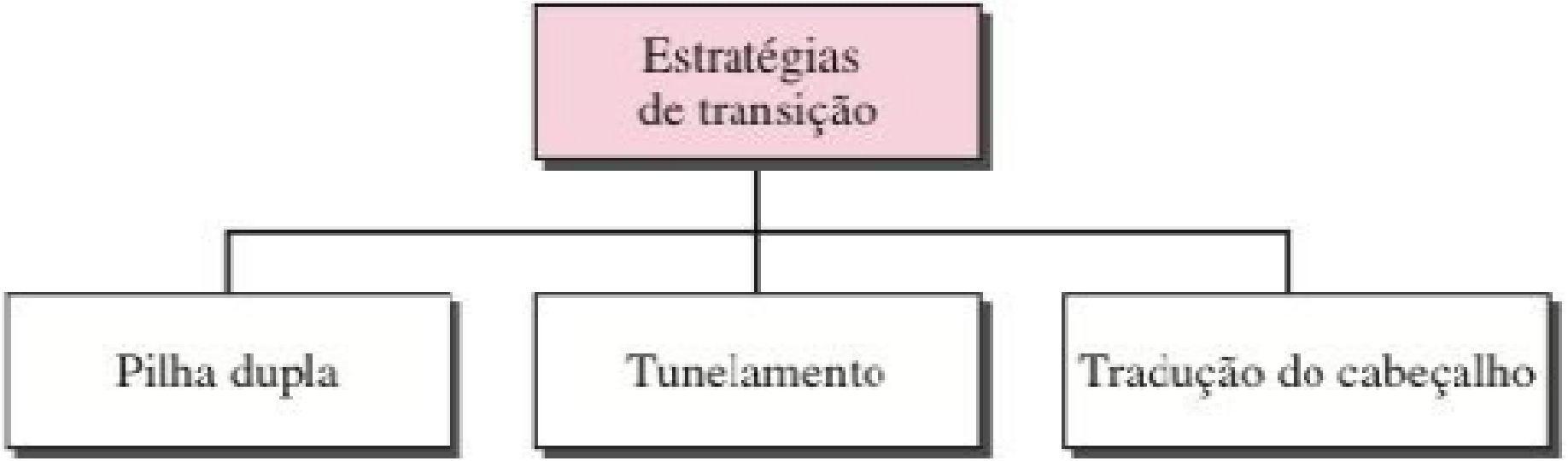


Figura 20.19 *Pilha Dupla*

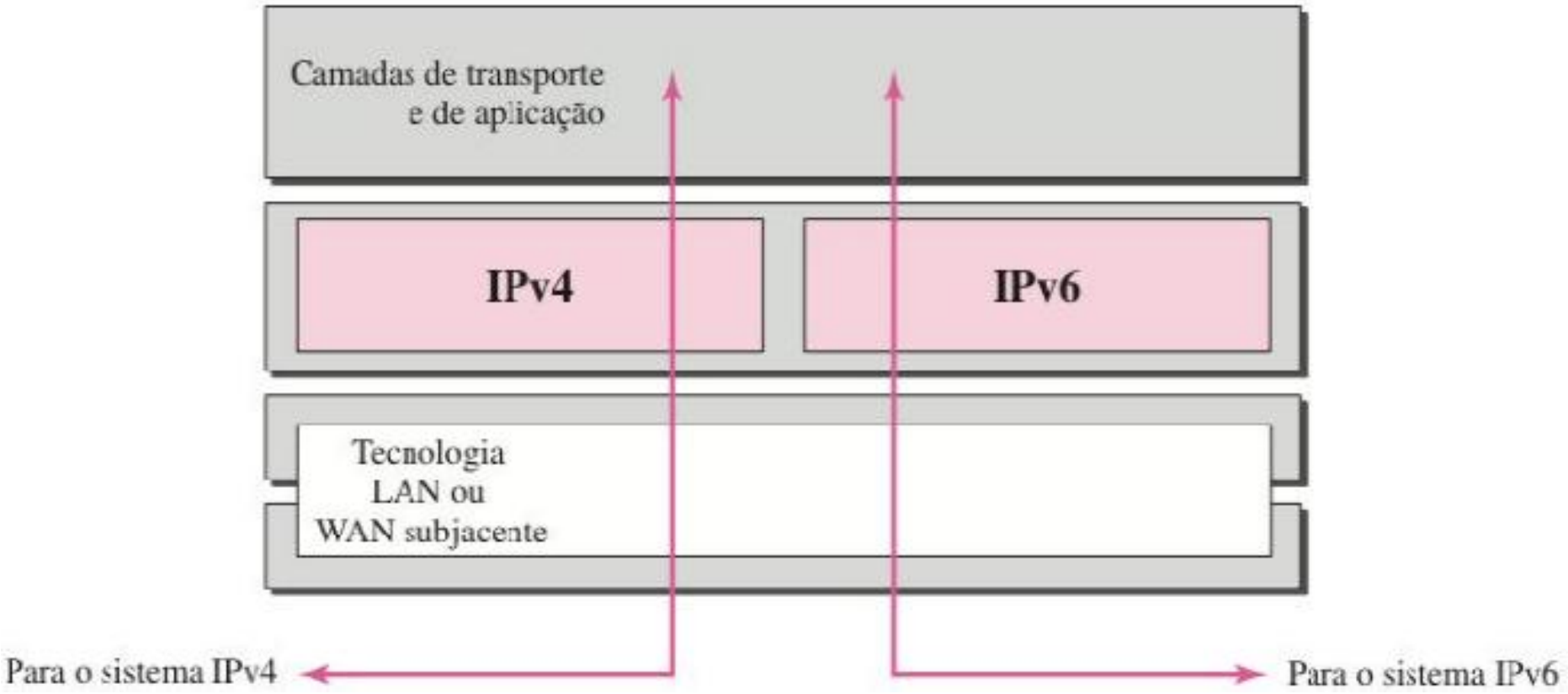


Figura 20.20 *Estratégia de Tunelamento*

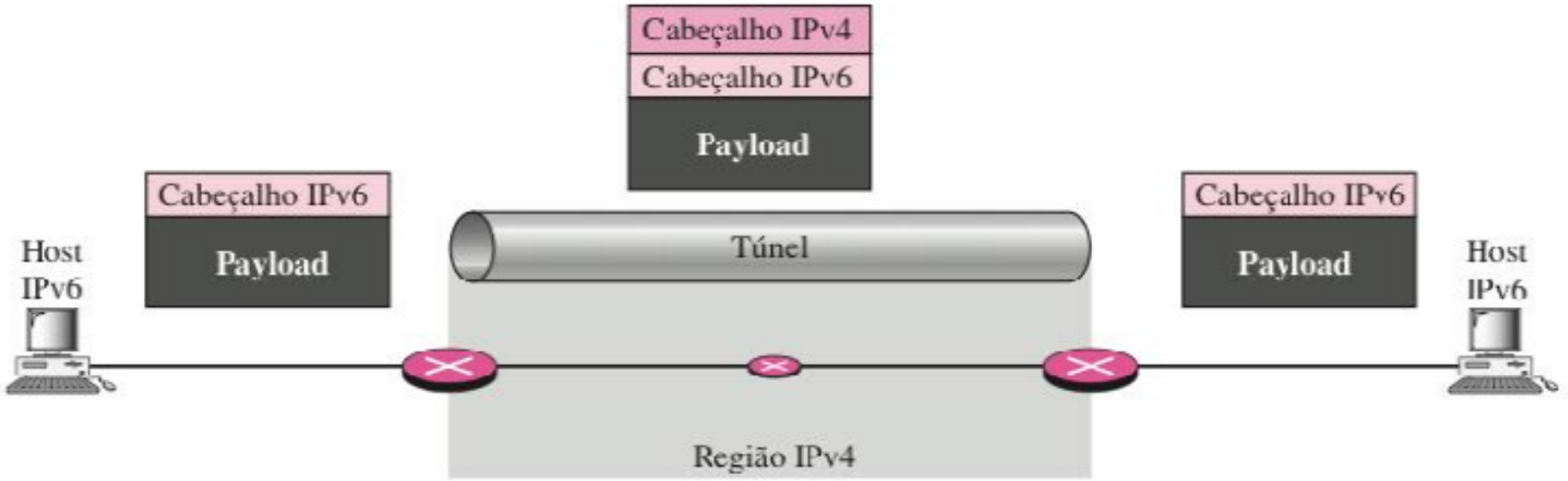


Figura 20.21 *Estratégia de Tradução do Cabeçalho*

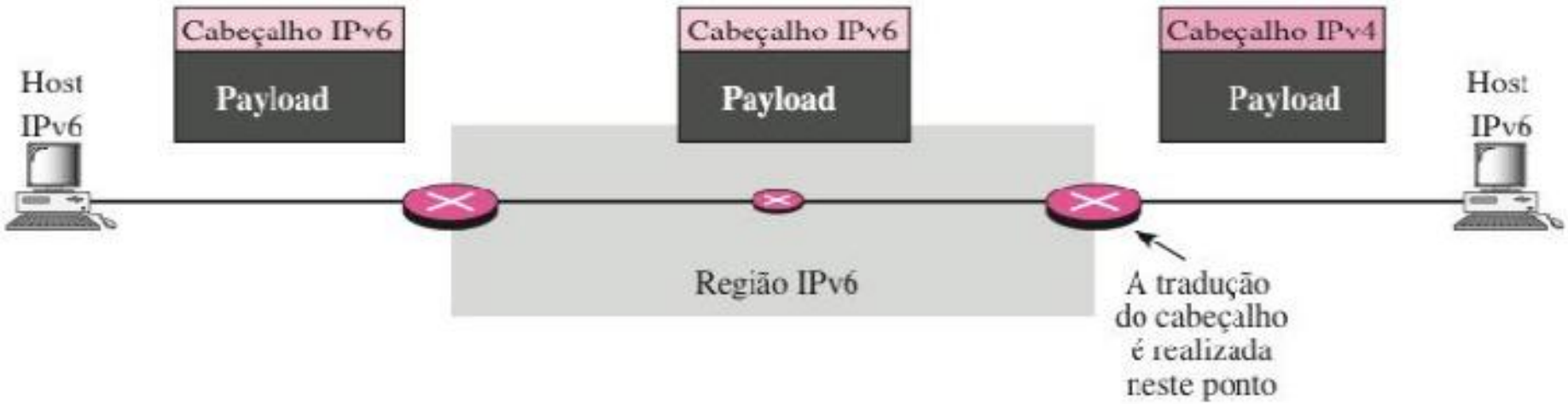


Tabela 20.11 *Tradução do Cabeçalhoc*

Procedimento para Tradução do Cabeçalho
1. O endereço associado IPv6 é convertido em um endereço IPv4 extraindo os 32 bits mais à direita.
2. O valor do campo de prioridade do IPv6 é descartado.
3. O campo tipo de serviço no IPv4 é configurado em zero.
4. O checksum do IPv4 é calculado e inserido no campo correspondente.
5. O rótulo de fluxo (flow label) do IPv6 é ignorado.
6. Cabeçalhos de extensão compatíveis são convertidos em opções e inseridos no cabeçalho IPv4. Alguns podem ser eliminados.
7. O comprimento do cabeçalho IPv4 é calculado e inserido no campo correspondente.
8. O comprimento total do pacote IPv4 é calculado e inserido no campo correspondente.