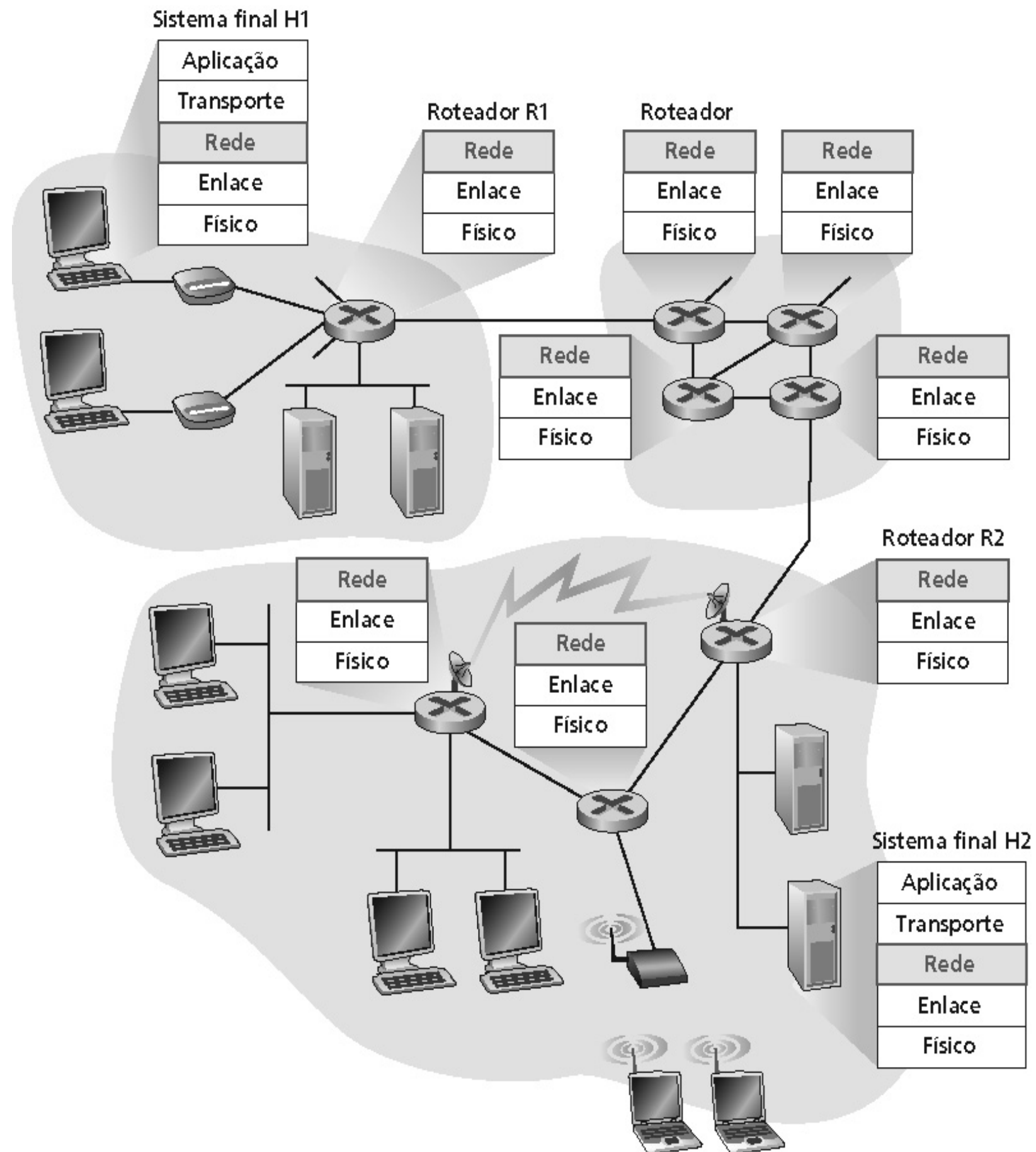
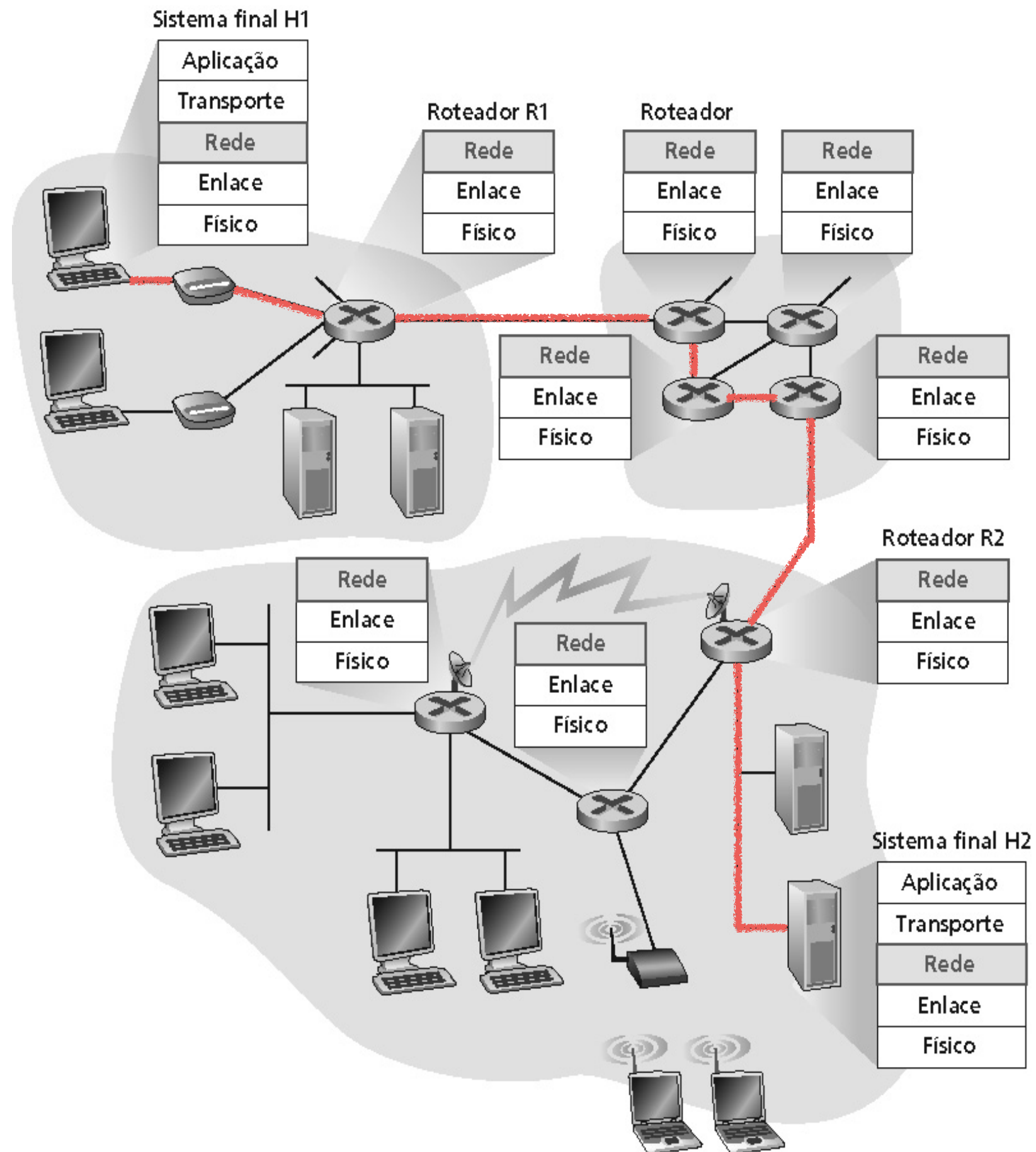


REDE DE COMPUTADORES

Camada de Redes





Prosseguindo os estudos, já vimos que cada camada prôve serviços para a camada superior e utiliza-se dos serviços fornecidos pelas camadas inferiores para enviar os dados de um lado para o outro. A camada de rede é responsável por:

- **Encapsulamento, Fragmentação, Roteamento, Endereçamento**

Ao fazer referência à camada de rede, chamamos esta PDU de **pacote**

- Transporta segmentos de informação da aplicação do *host* transmissor para a aplicação do *host* receptor.
- No lado transmissor encapsula os segmentos em datagramas.
- No lado receptor, entrega os segmentos à camada de transporte.
- Existem protocolos da camada de rede em cada *host* e nos roteadores.
- Roteador é o elemento característico da camada de rede.
- O Roteador examina os campos de cabeçalho em todos os datagramas IP que passam por ele e decide para onde enviar.

Encapsulamento

- consiste no encapsulamento da carga útil (**payload**) em um pacote da camada de rede na origem e o desencapsulamento no destino, não havendo a utilização o **payload**, nem a alteração do seu conteúdo.
- A única alteração possível é a fragmentação do pacote. Caso o pacote seja fragmentado, a camada de rede é a encarregada de aguardar o recebimento de todos, reorganizá-los e entregar para a camada superior.

Roteamento

- O **Roteamento** é um serviço considerada tão importante quanto o Empacotamento.
- É a tarefa de encontrar a melhor rota entre a origem e o destino, pois como estudamos, existem diversas rotas de diferentes tipos de tecnologias entre a origem e o destino.
- O roteamento utiliza-se de alguns protocolos de roteamento, que mapeia os vizinhos e possui algumas políticas para manter a lista sempre atualizado.

Encaminhamento

- É a ação propriamente dita que o cada roteador toma baseado na **tabela de roteamento** ou **tabela de encaminhamento**.
- Quando um datagrama é recebido, ele deve encaminhar para a rede **unicast** ou as redes **multicast** as quais ele esta conectado.
- O roteador acessa o cabeçalho para buscar o endereço de destino ou alguma outra informação, para determinar o interface de saída correspondente na **tabela de roteamento**.

Controle de erros

- Como o datagrama pode ser fragmentado em cada roteador, a verificação de erros se torna ineficiente
- MAS, existe um ***checksum*** do cabeçalho, para controle e prevenção de erros.

Controle de fluxo

- **Não há!**

Controle de congestionamento

- É um problema quando o roteador começa a descartar muitos pacotes;

Qualidade de serviço

- A qualidade de serviço (***QoS - Quality of Service***) busca atender as diversas formas de aplicações e conteúdos (vídeo, voz, imagens, texto)
- Efetivamente não foi tão adotada na camada de rede, deixando para a camada de aplicação.

Segurança

- Não era uma preocupação no início, devido ao número pequeno de usuários, por isto foi projetada sem funcionalidades de segurança
- Hoje, entretanto, a segurança é vital! Camadas superiores implementam protocolos de segurança, e **IPSec**.

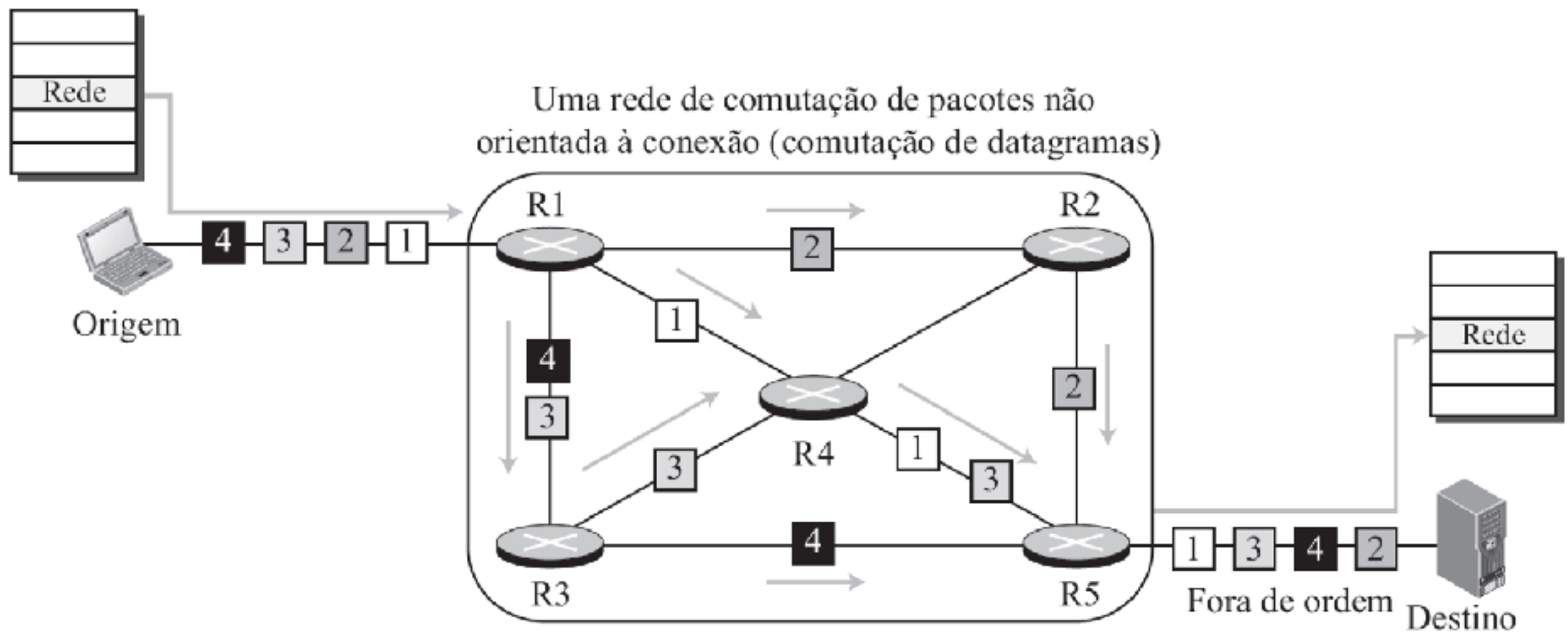
Comutação

- O roteador cria uma ligação entre uma porta de entrada e uma(s) porta(s) de saída(s)
 - **Comutação de circuitos**
 - **Comutação de pacotes**
- A origem envia uma mensagem que é fragmentada em diversos pacotes, e o destino recebe um a um, e aguarda todos os pacotes de uma mesma mensagem para repassar para camada superior.

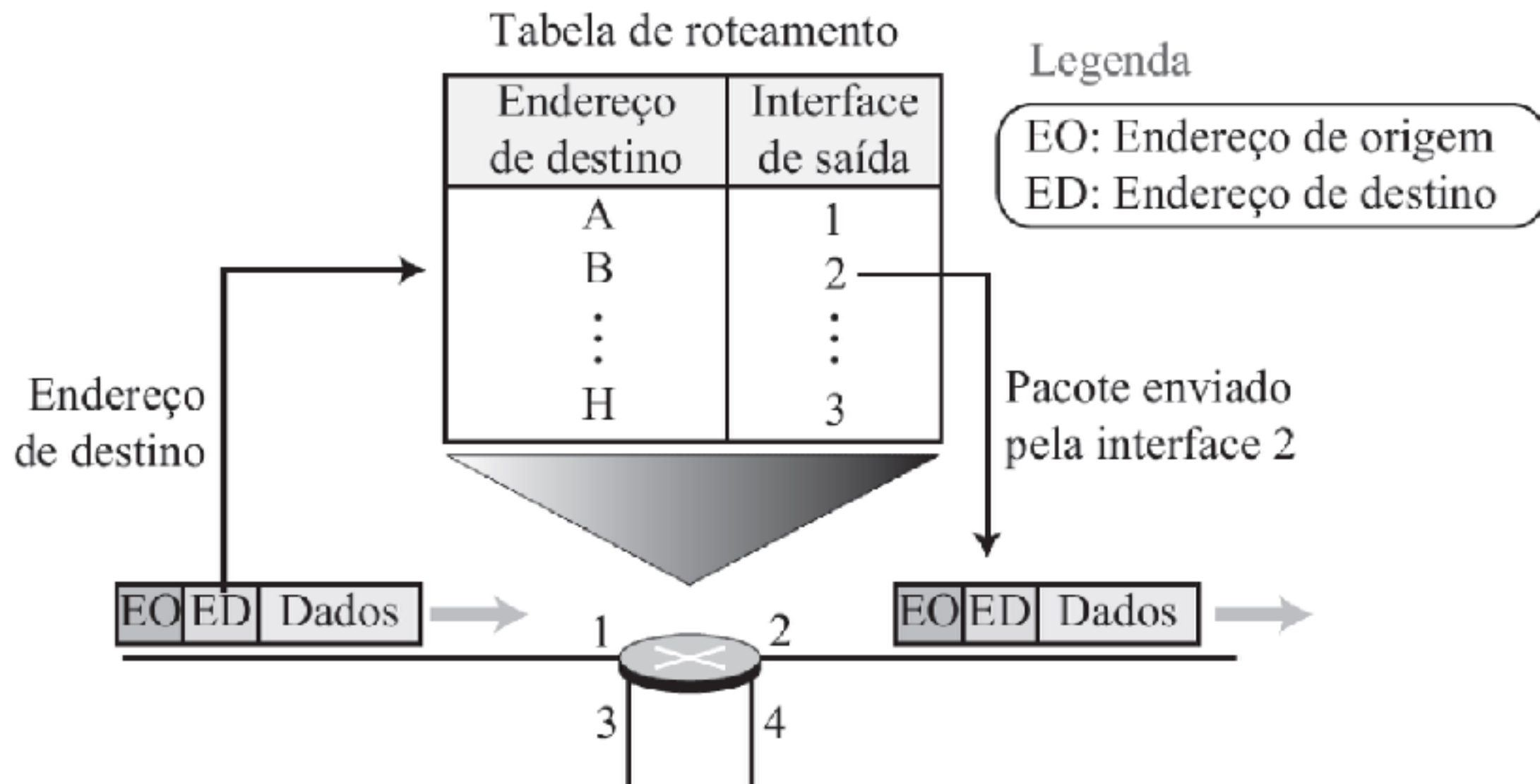
Comutação de pacotes

- é um **serviço não orientado à conexão**, e foi a maneira como a camada de rede foi projetada
- cada pacote é tratado de forma independente, eles podem ou não percorrer o mesmo caminho
- Um pacote ainda pode ser sucedido por outro pacote da mesma mensagem ou uma mensagem diferente
- Cada pacote é analisado através do cabeçalho, utilizando os endereços de origem e destino

Comutação de pacotes



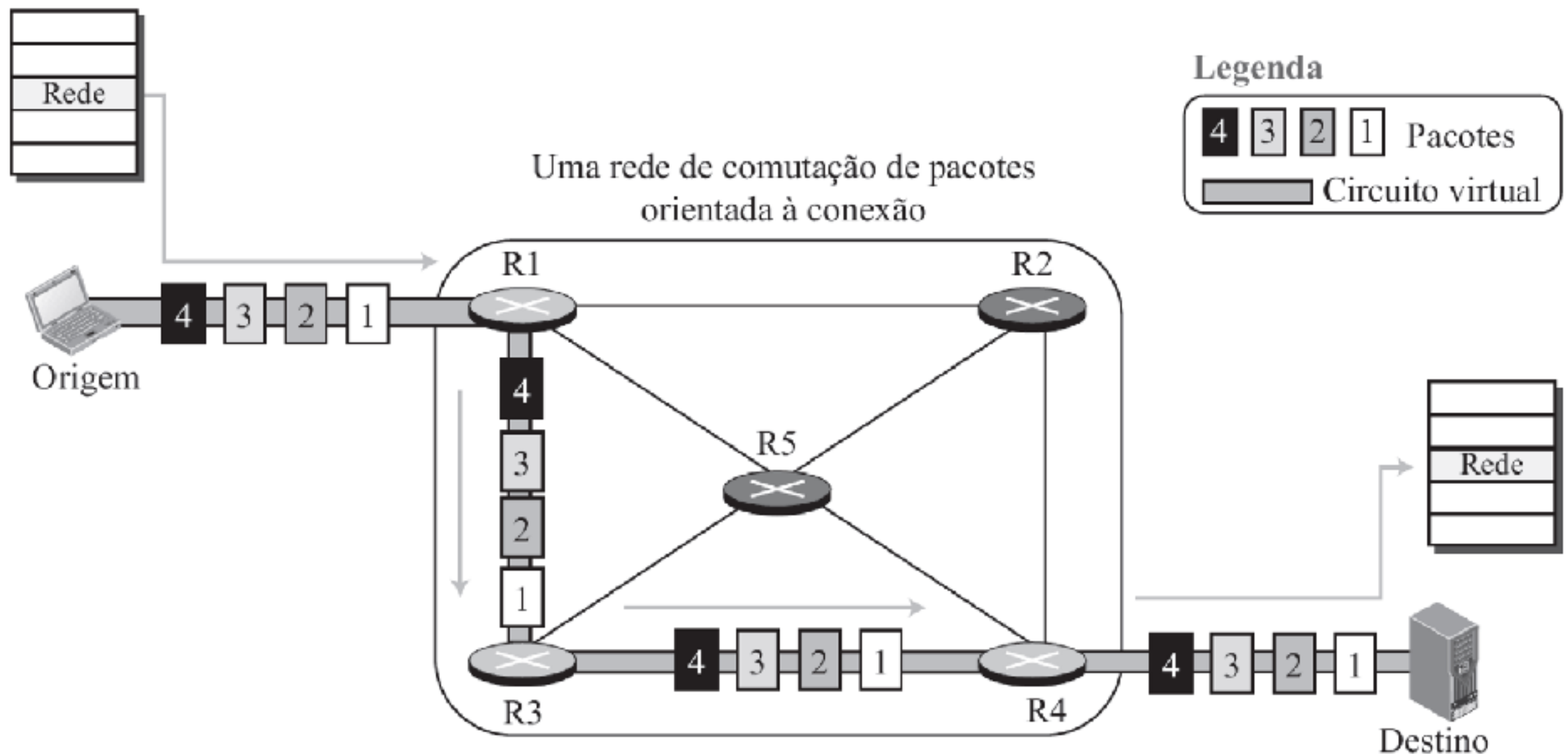
Comutação de pacotes



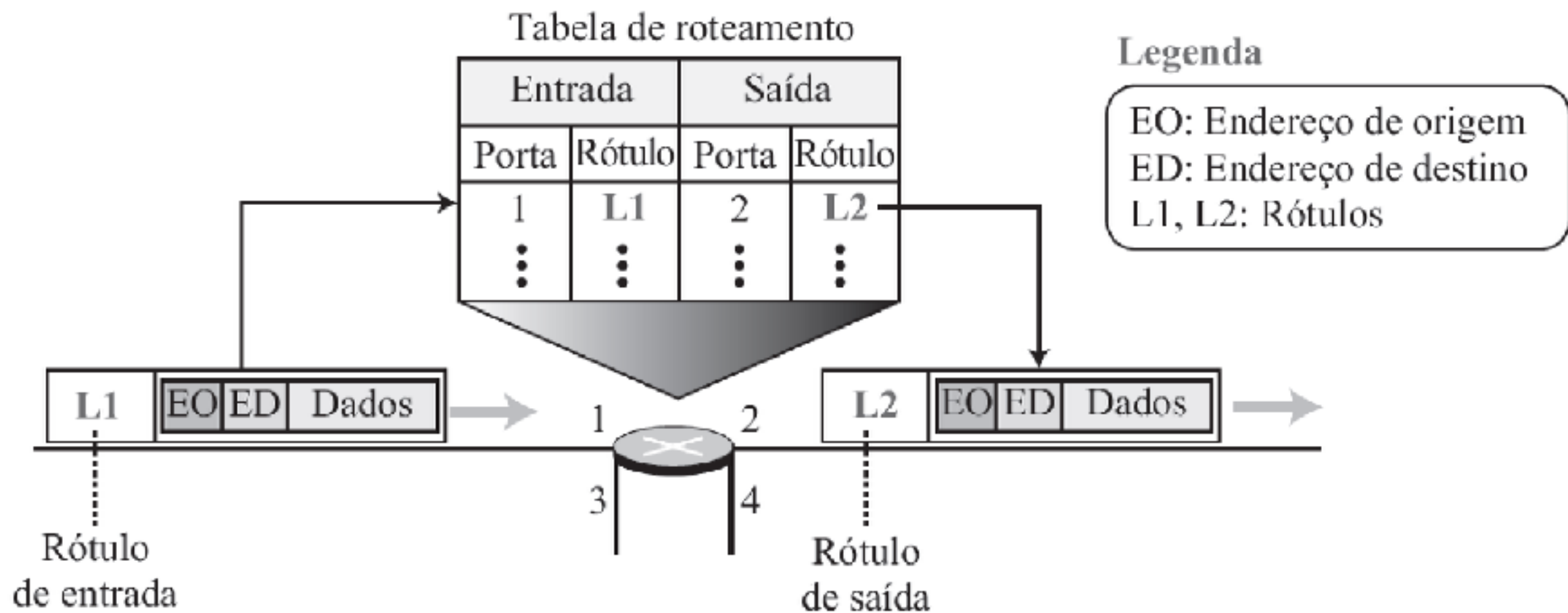
Comutação de circuitos

- é um **serviço orientado à conexão**
- existe uma relação entre os pacotes pertencentes a uma mesma mensagem
- antes do envio dos datagramas de uma mensagem, é necessário a configuração do caminho
- Cada pacote é encaminhado de acordo com o rótulo

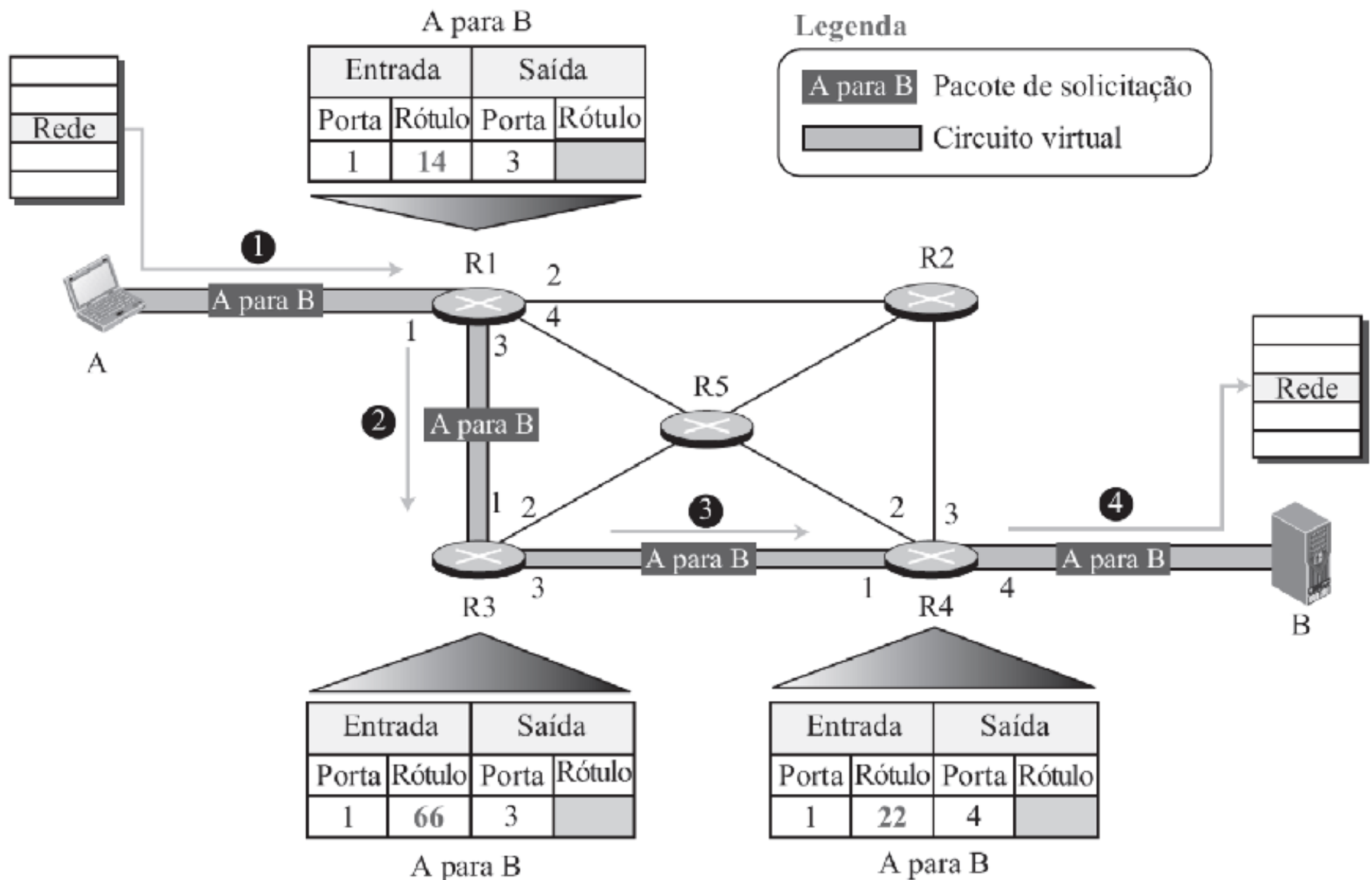
Comutação de circuitos



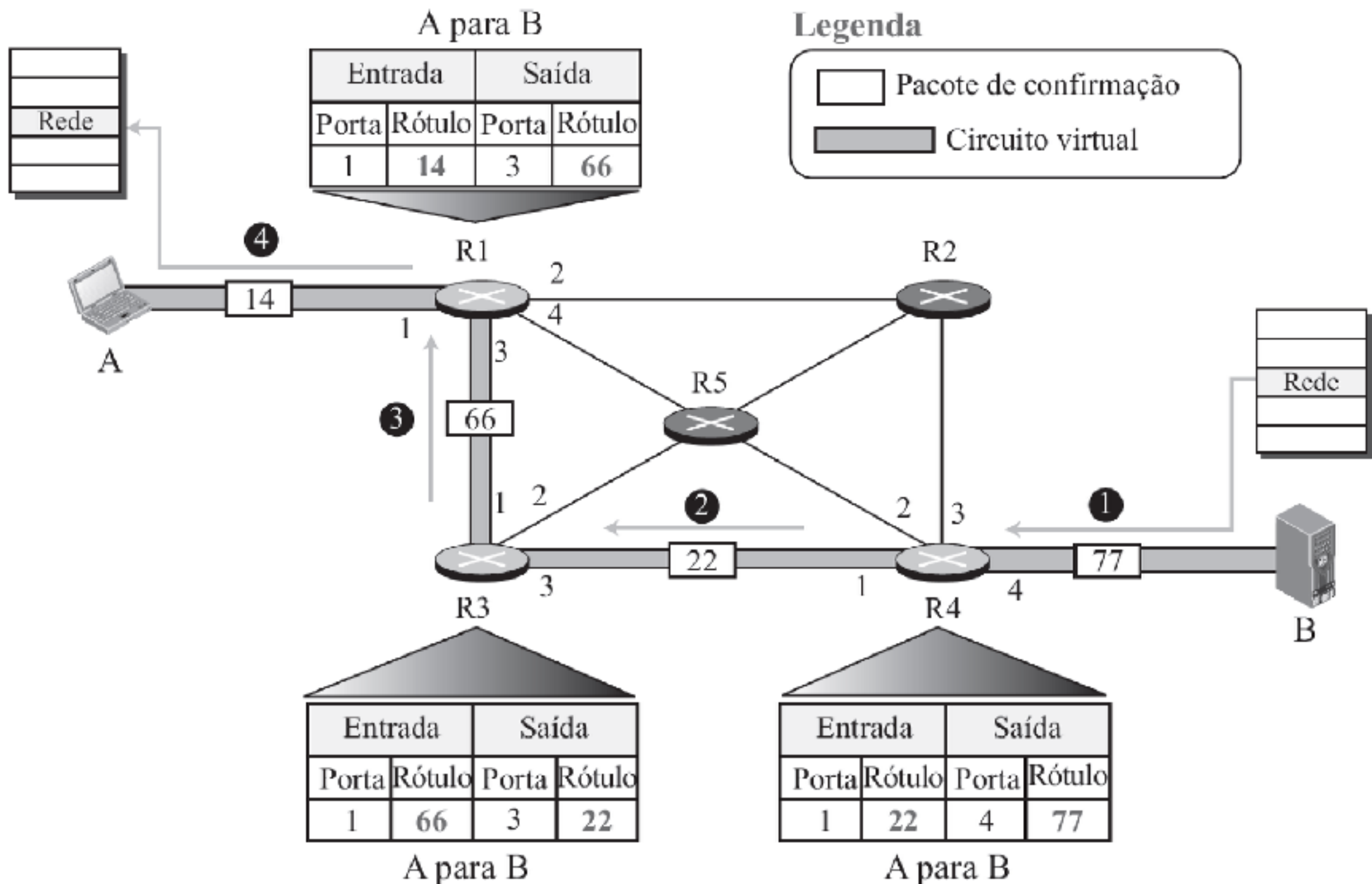
Comutação de circuitos



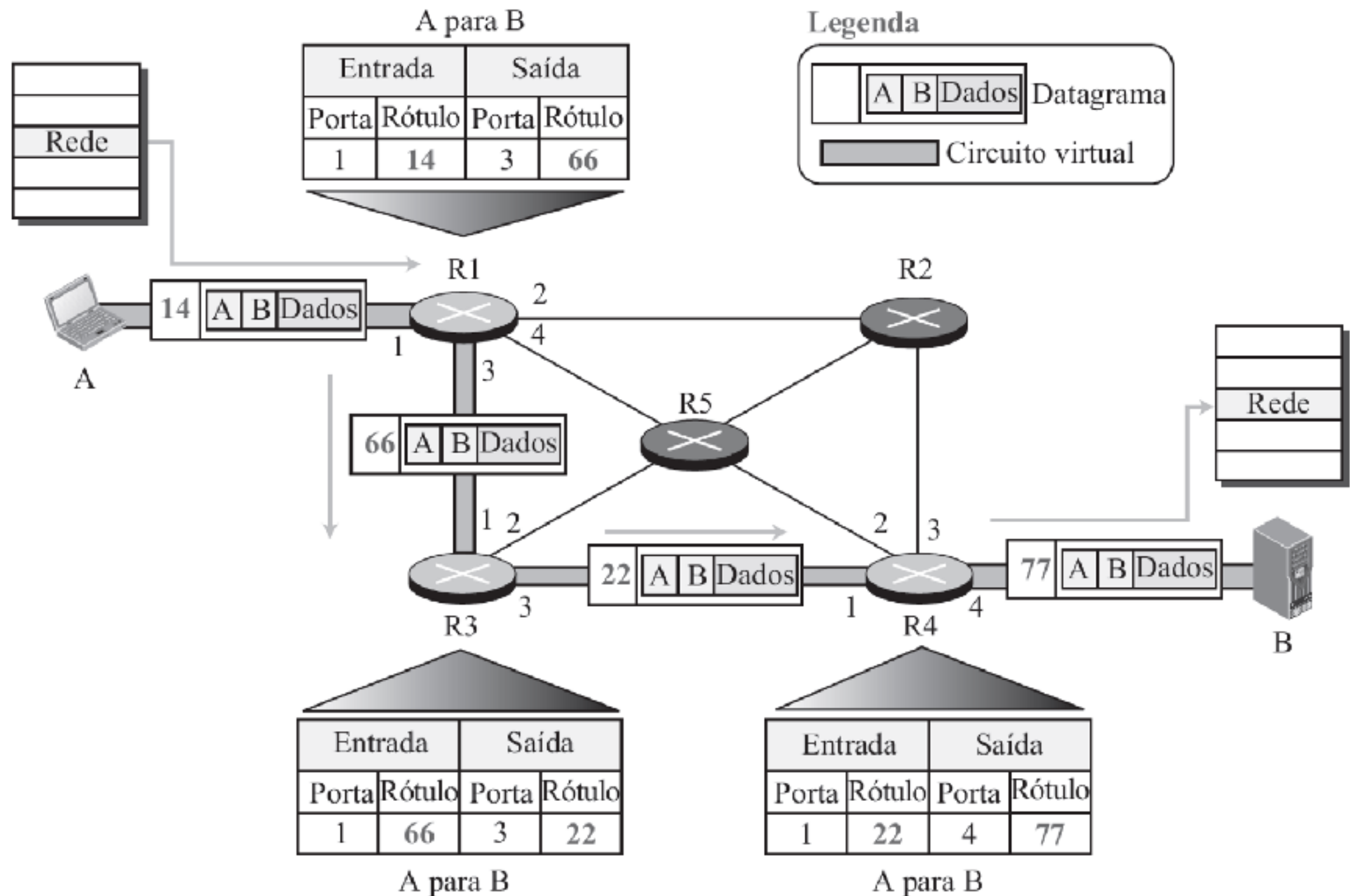
Comutação de circuitos



Comutação de circuitos



Comutação de circuitos



Desempenho

Desempenho

- Medimos o desempenho através:
 - **atraso**
 - **vazão**
 - **perda de pacotes**

Atraso

- Atraso transmissão
- Atraso de propagação
- Atraso de processamento
- Atraso de fila

Atraso de transmissão

Mede o tempo de transmissão do 1o bit até o último bit do pacote. É maior para pacotes maiores, e menor para pacotes menores.

$$\text{Atraso} = (\text{tam do pacote}) / (\text{tx de transmissão})$$

Por exemplo, rede cabeada ethernet, com uma taxa de 100 Mbits/s para um pacote de 10.000 bits

$$10000/100000000 = 1/10000 \text{ s} = 0,0001 \text{ s}$$

Atraso de propagação

É tempo que um bit leva para viajar do ponto A ao ponto B no meio de transmissão. O atraso depende da velocidade de propagação do meio de transmissão em relação e da distância.

$$\text{Atraso} = (\text{Distância}) / (\text{Vel. de propagação})$$

Por exemplo, em uma WAN ponto a ponto tiver a distância de 2km e a velocidade de propagação dos *bits* for 2×10^8 metros/segundo.

$$2000 / 2 \times 100000000 = 1 / 10000 \text{ s} = 0,0001 \text{ s}$$

Atraso de processamento

É o tempo necessário para o roteador ou um *host* de destino leva para receber o pacote, processar o cabeçalho e dar uma destinação, repassar a informação para a camada superior ou rotear.

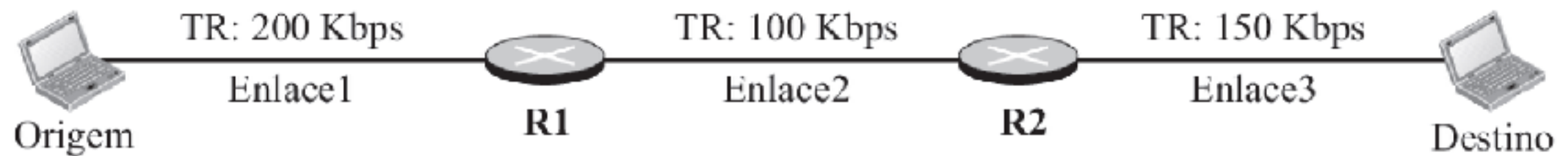
Atraso de fila

Acontece geralmente no roteador, é o tempo que o pacote deve aguardar na fila de entrada ou saída para ser tratado.

Vazão

É definida como o número de *bits* que passar por um ponto em um segundo, correspondendo na realidade, à taxa de transmissão de dados naquele ponto.

Vazão



(a) Um caminho envolvendo três enlaces

TR: Taxa de transmissão



(b) Simulação usando tubos

Perda de pacotes

Um roteador recebe um pacote, e enquanto ele processa, outros pacotes são recebidos. Estes são armazenados no *buffer*, que possui um tamanho limitado.

Uma vez cheio o buffer, os pacotes começam a ser descartados. Isto faz com que aconteça o reenvio dos pacotes, aumentando o tráfego, e consequentemente perdendo mais pacotes.

Congestionamento

Controle de congestionamento

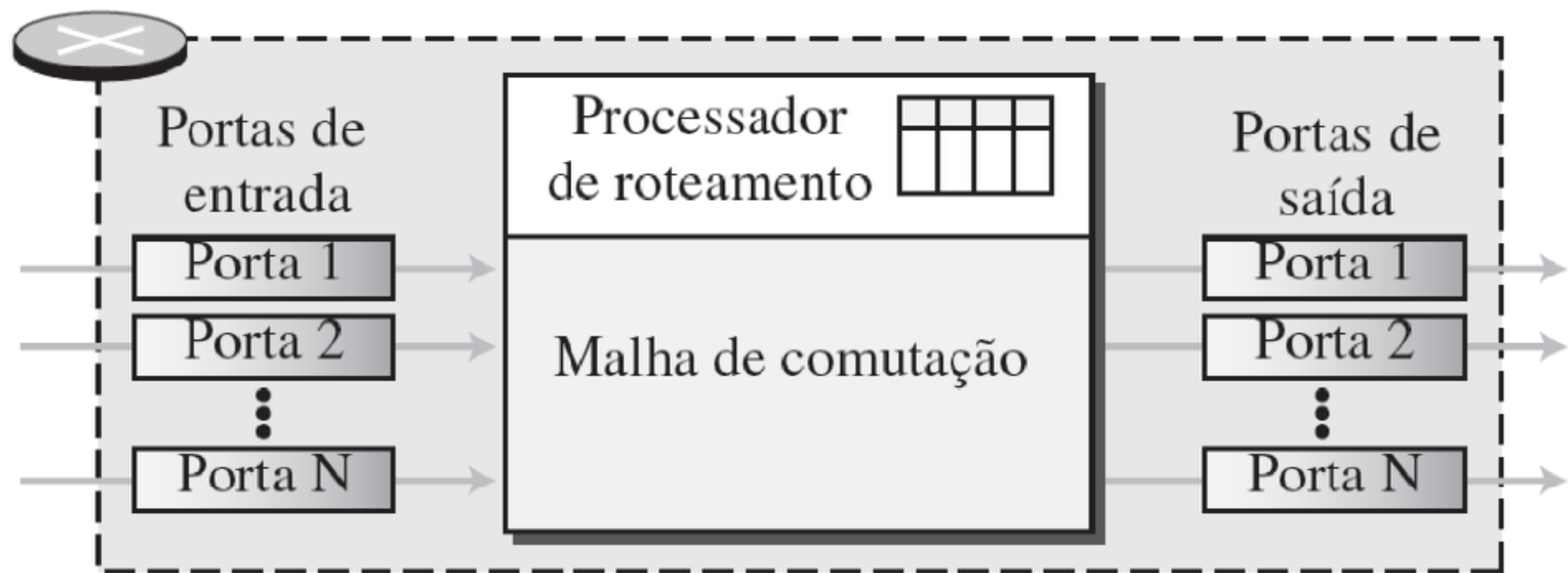
O controle de congestionamento consiste em técnicas e mecanismos para **evitar** ou **eliminar** o congestionamento.

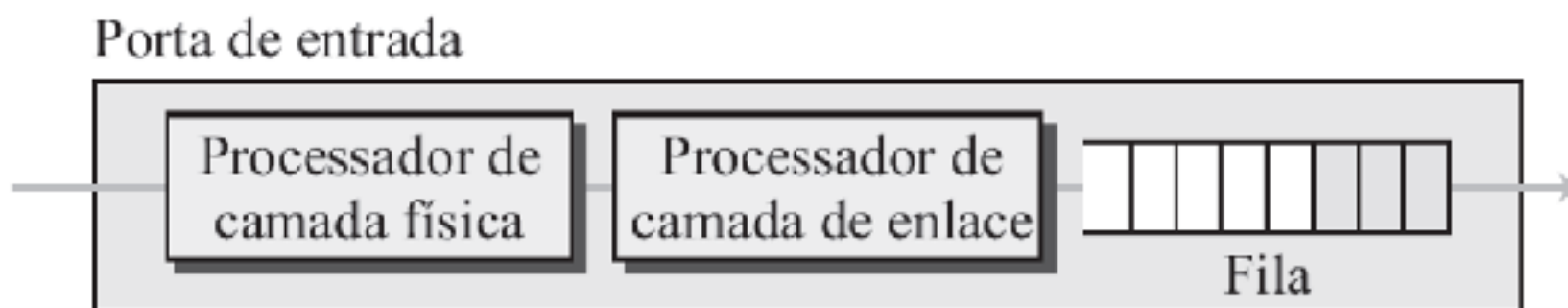
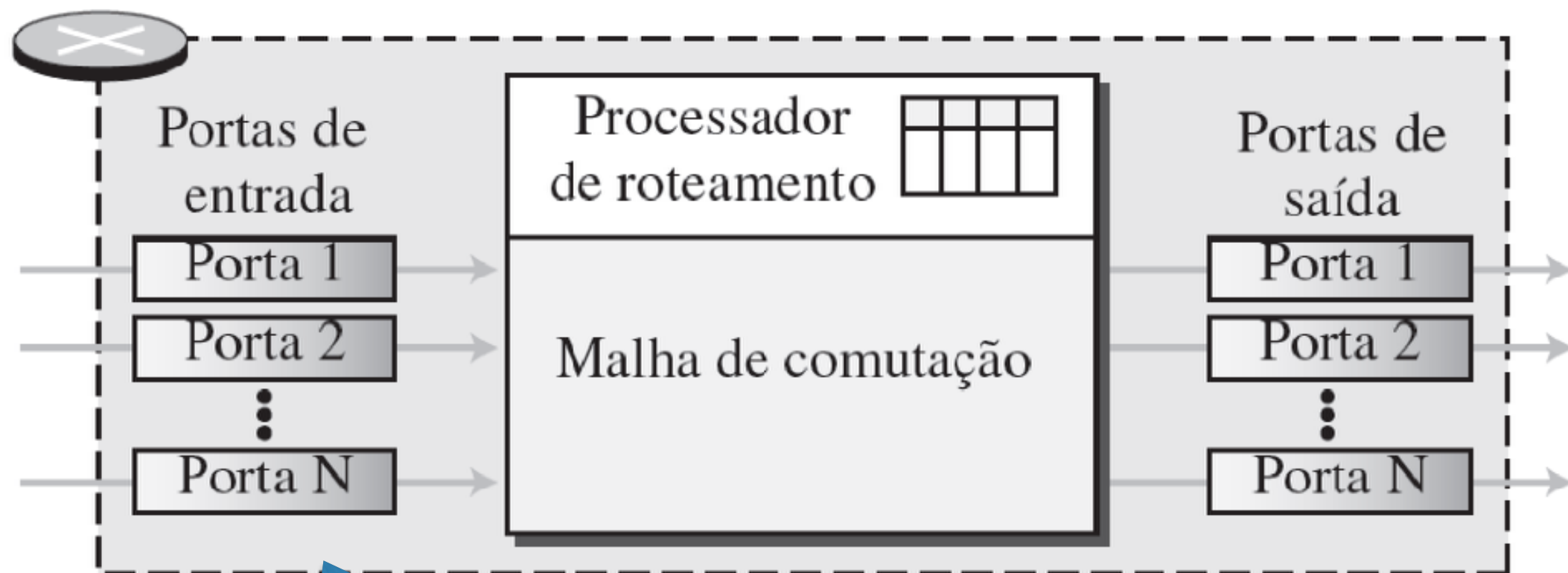
Controle de congestionamento

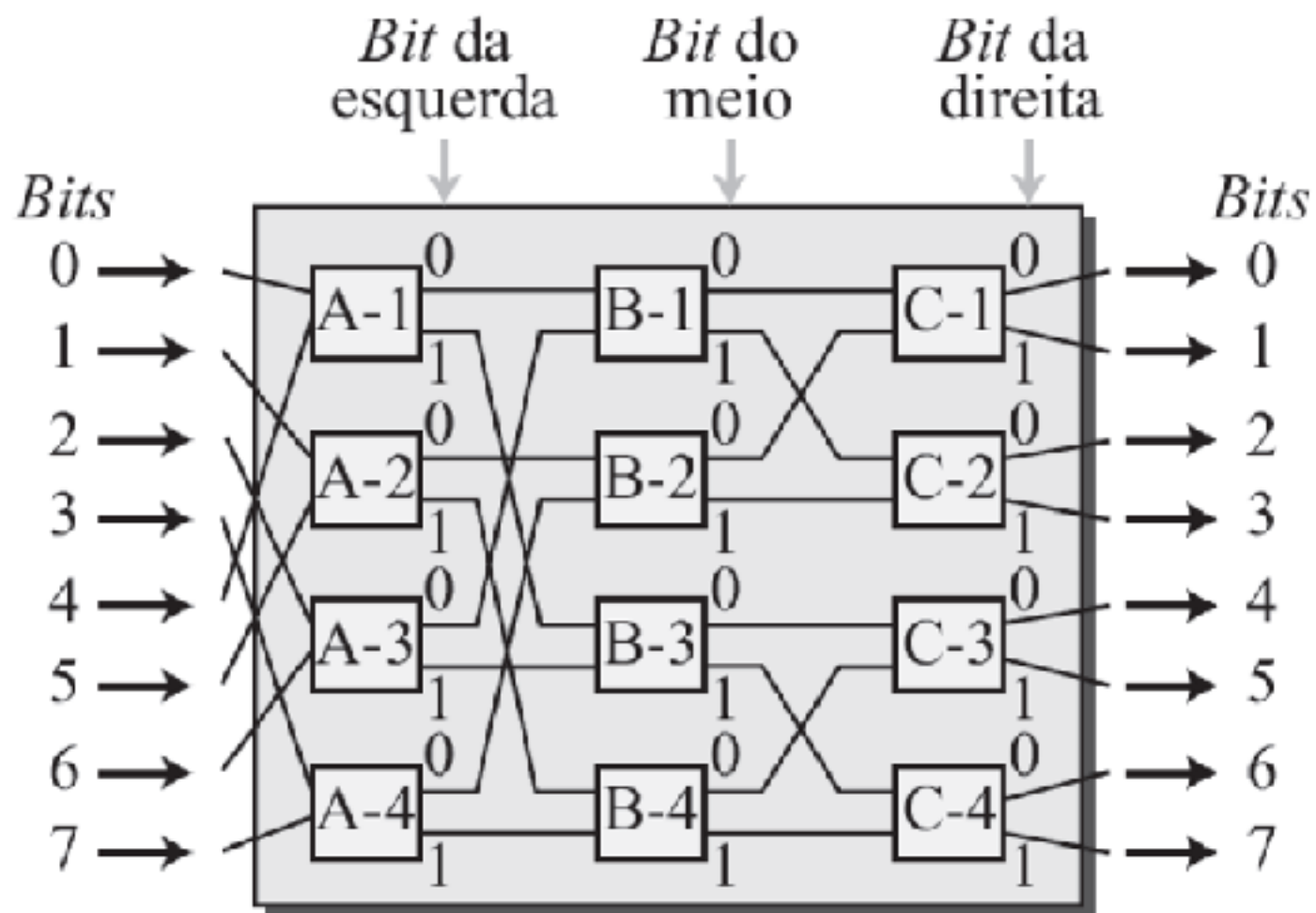
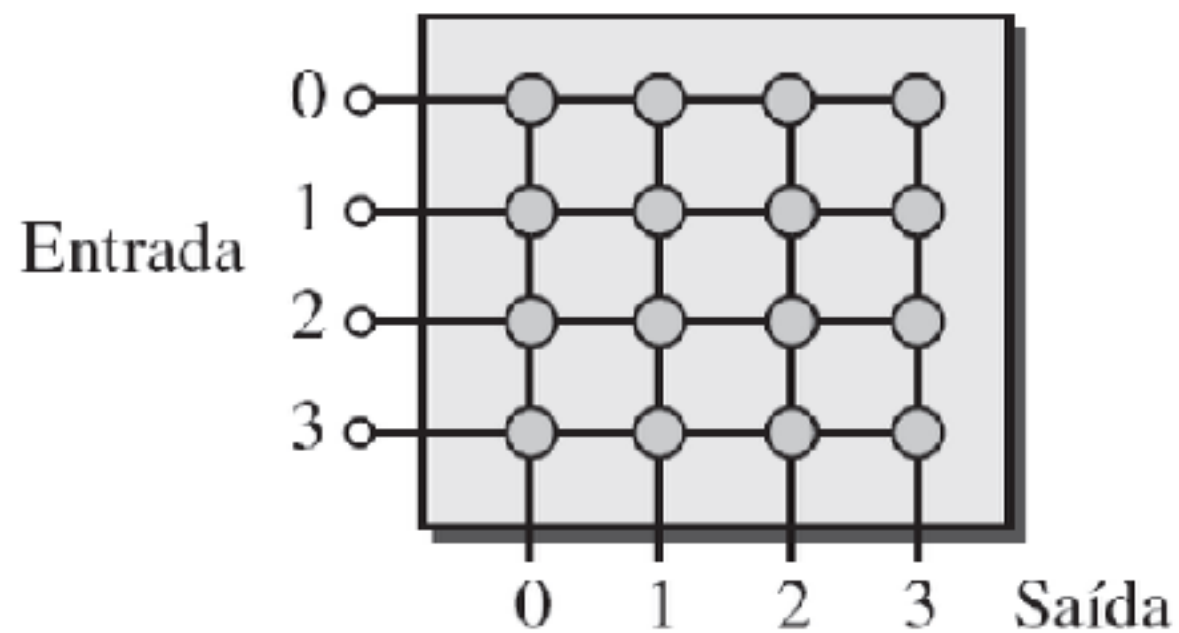
Política de retransmissão

Retransmissão é inevitável

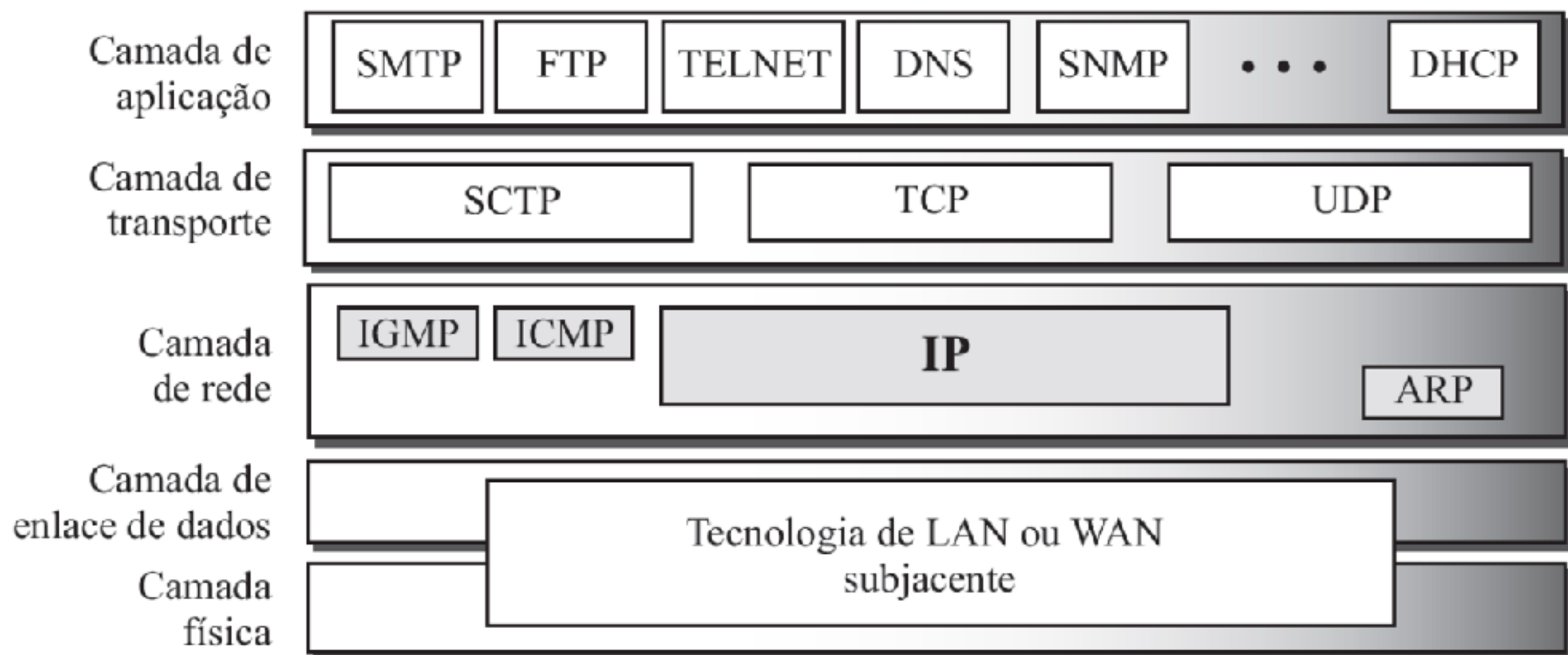
Roteador







Protocols



Internet Protocol - IP

- O **Internet Protocol**, ou simplesmente **IP**, é um protocolo da camada de rede responsável pelo encaminhamento dos dados numa rede.
- É o protocolo base da arquitetura da Internet e é utilizado pelos serviços de aplicação (páginas web, e-mail, transferência de arquivos, gerência de redes, resolução de nomes, dentre outros.)

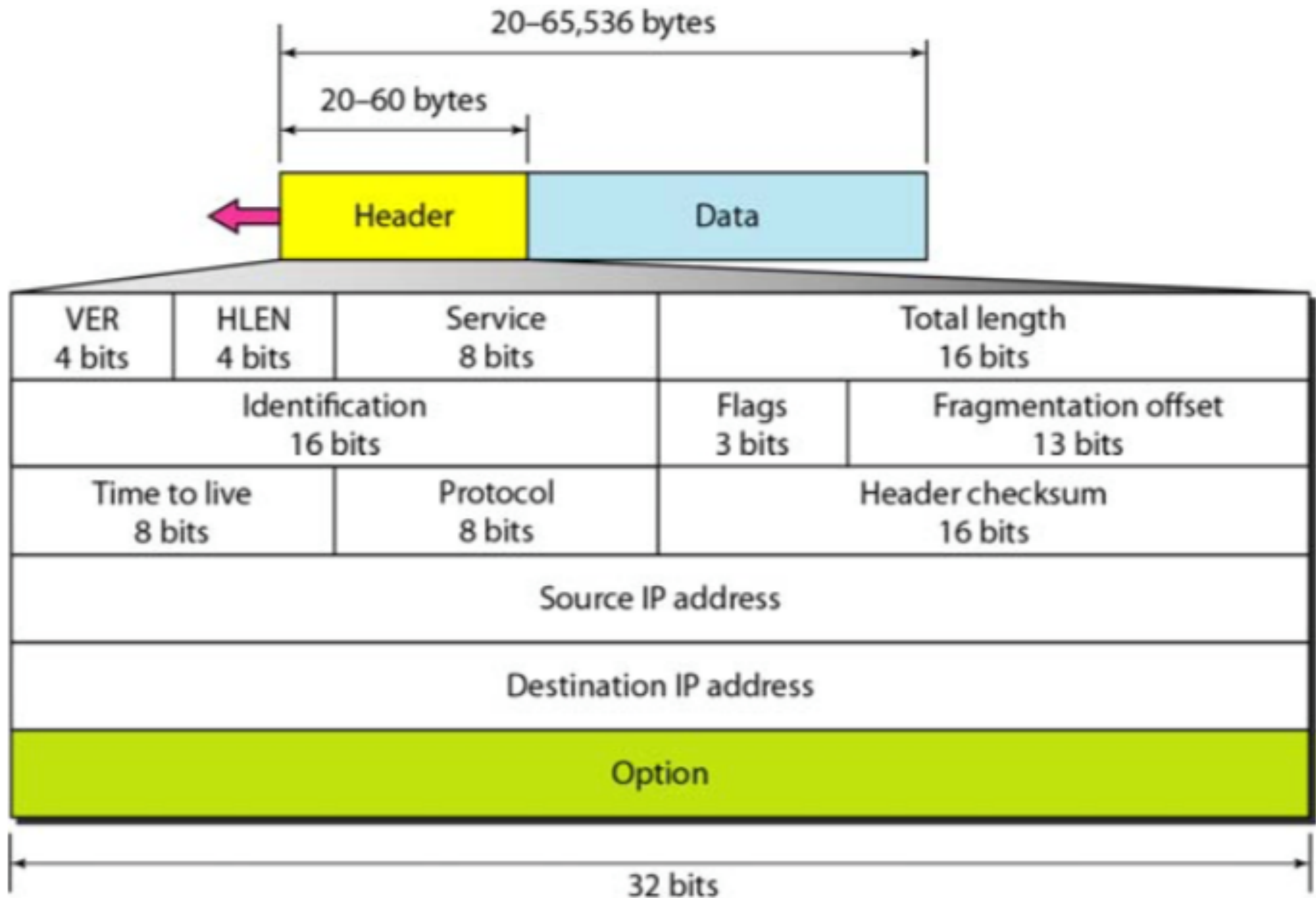
Internet Protocol - IP

A summary of the contents of the internet header follows:

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
+--+																																							

Example Internet Datagram Header

Internet Protocol - IP



Internet Protocol - IP

RFC 791,...

VER – informa a versão do protocolo.

HLEN – informa o tamanho do cabeçalho

Service – tem como objetivo identificar o tipo de serviço para dar preferência no roteamento. Entretanto não foi muito utilizado.

TTL – indica a quantidade de hops entre transmissor e receptor. O valor é decrementado a cada roteador do caminho.

Source IP e **Destination IP** – indica os endereços origem e destino.

Checksum – serve para verificar a integridade do cabeçalho IP.

Internet Protocol - IP

Endereçamento IP

Cada computador conectado a Internet possui um endereço IP único e universal composto de **32 bits** e pode ser escrito da seguinte forma:

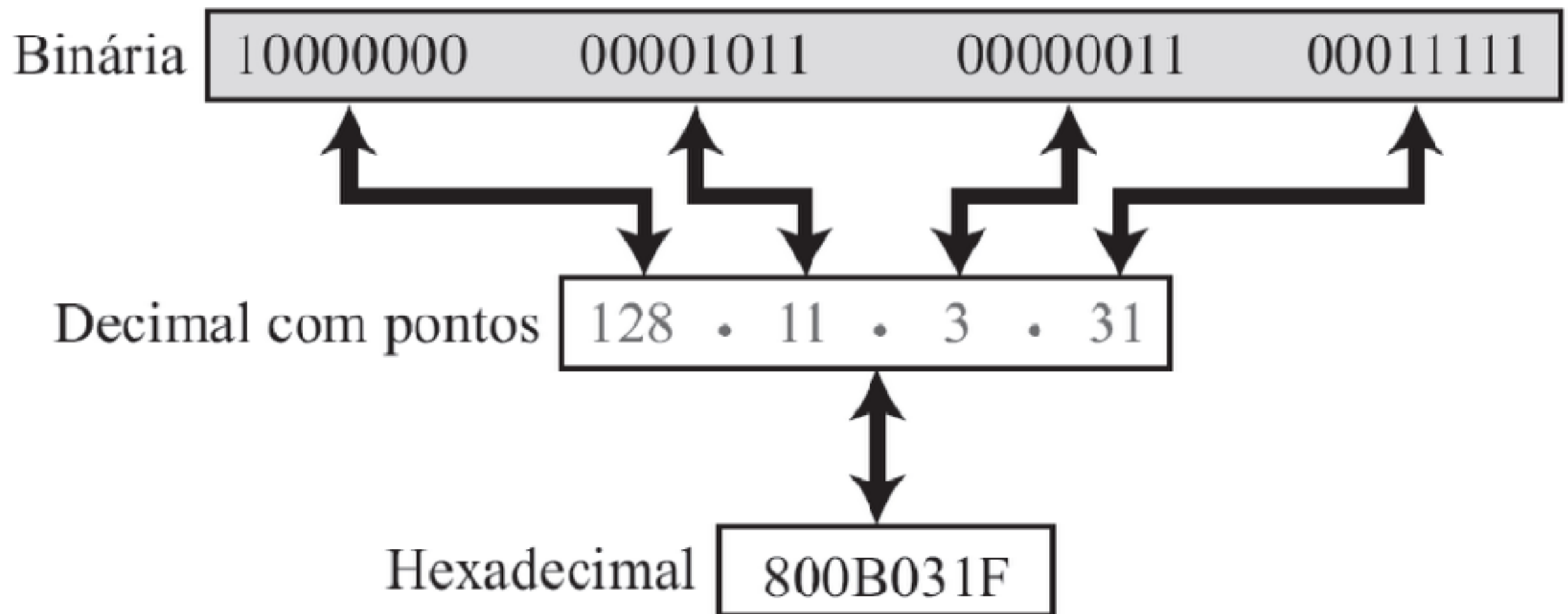
187.45.190.82

Tal endereço também pode ser escrito com a seguinte notação binária:

10111011.00101101.10111110.01010010

Diferentemente do **MAC Address** o endereço IP é configurado via software e pode ser alterado pelo usuário e/ou administrador da rede.

Internet Protocol - IP



Internet Protocol - IP

Endereçamento IP

Para a configuração do endereço IP devemos também levar em consideração:

Mascara – Uma máscara de subrede (subnet mask ou netmask) é um número de 32 bits usada para separar em um IP a parte correspondente à rede pública, à subrede e aos hosts.

Gateway – é um dispositivo intermediário geralmente destinado a interligar redes servindo de caminho para elas. Pode também separar domínios de colisão ou mesmo traduzir protocolos. Exemplos: roteadores, firewalls e proxy.

Internet Protocol - IP

Inicialmente, estes endereços foram divididos em três classes de tamanhos fixos da seguinte forma:

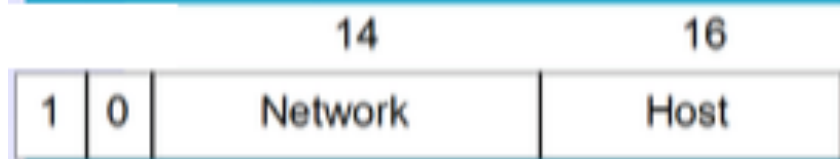
- **Classe A:** definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0;
- **Classe B:** definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0;
- **Classe C:** definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0;

Internet Protocol - IP

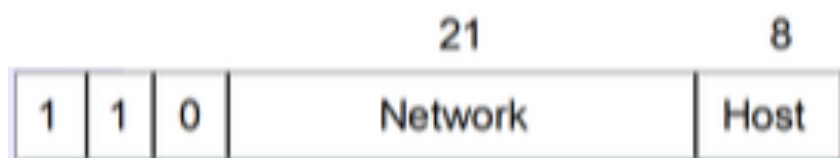
Classe	Formato	Redes	Hosts
A	7 bits Rede, 24 bits Host	128	16.777.216
B	14 bits Rede, 16 bits Host	16.384	65.536
C	21 bits Rede, 8 bits Host	2.097.152	256



Classe A (máscara: 255.0.0.0) -----> 126 redes, 16.777.214 hosts/rede



Classe B (máscara: 255.255.0.0) -----> 16.384 redes, 65.534 hosts/rede



Classe C (máscara: 255.255.255.0) ----> 2.097.152 redes, 254 hosts/rede

Internet Protocol - IP

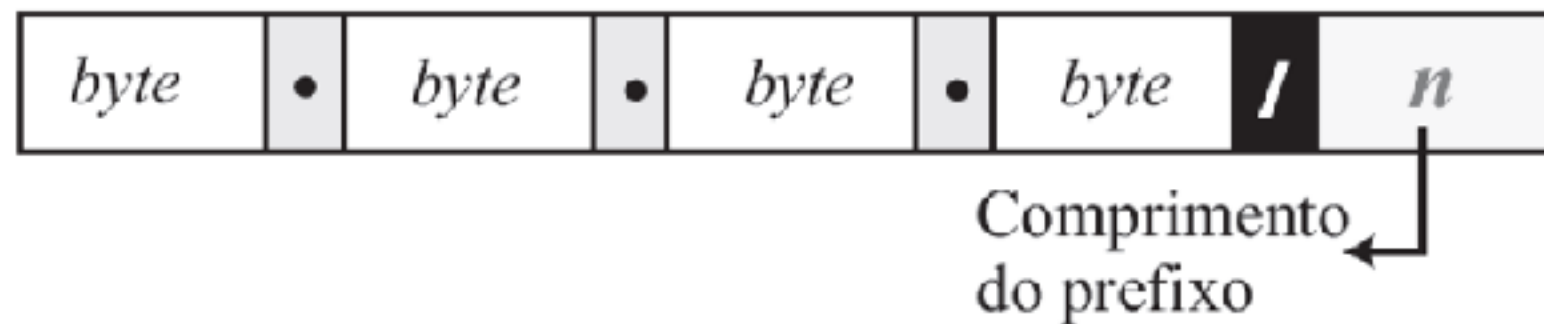
Classes Reservadas

Existem classes de endereços reservadas que não podem ser consideradas como endereçáveis para acesso na internet, como:

- **127.0.0.0/8** – IP de loopback1
- **0.0.0.0** – Identificador da rede
- **255.255.255.255** – IP de broadcast (todas as redes)
- **10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16** – Exemplos de IPs para redes privadas.

Internet Protocol - IP

Notação de barra ou *Classless Inter-Domain Routing* - (CIDR)



Exemplos:

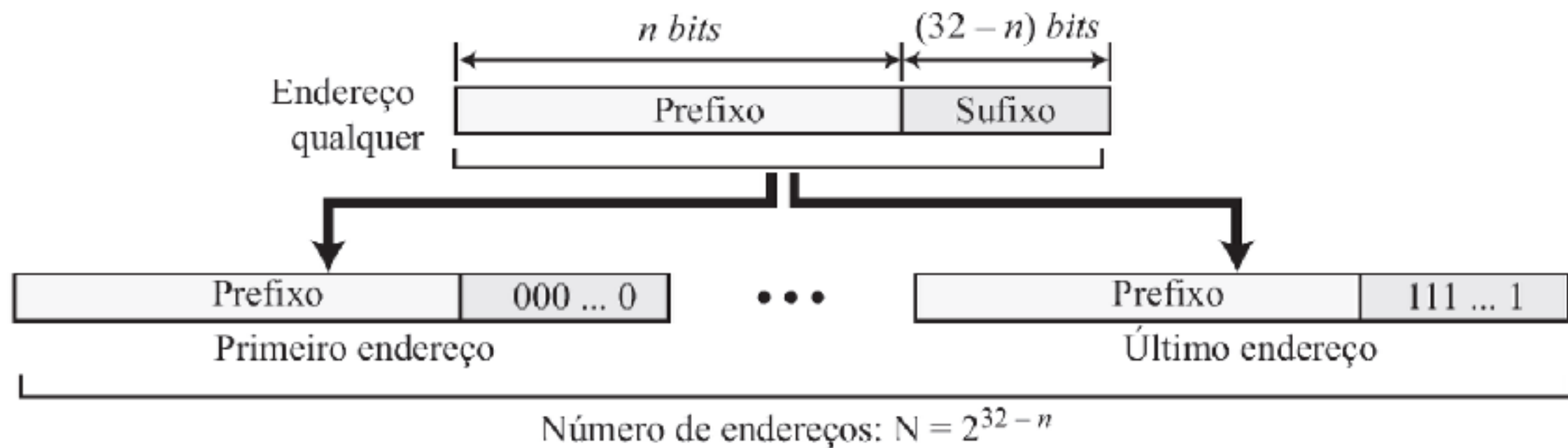
12.24.76.8/8

23.14.67.92/12

220.8.24.255/25

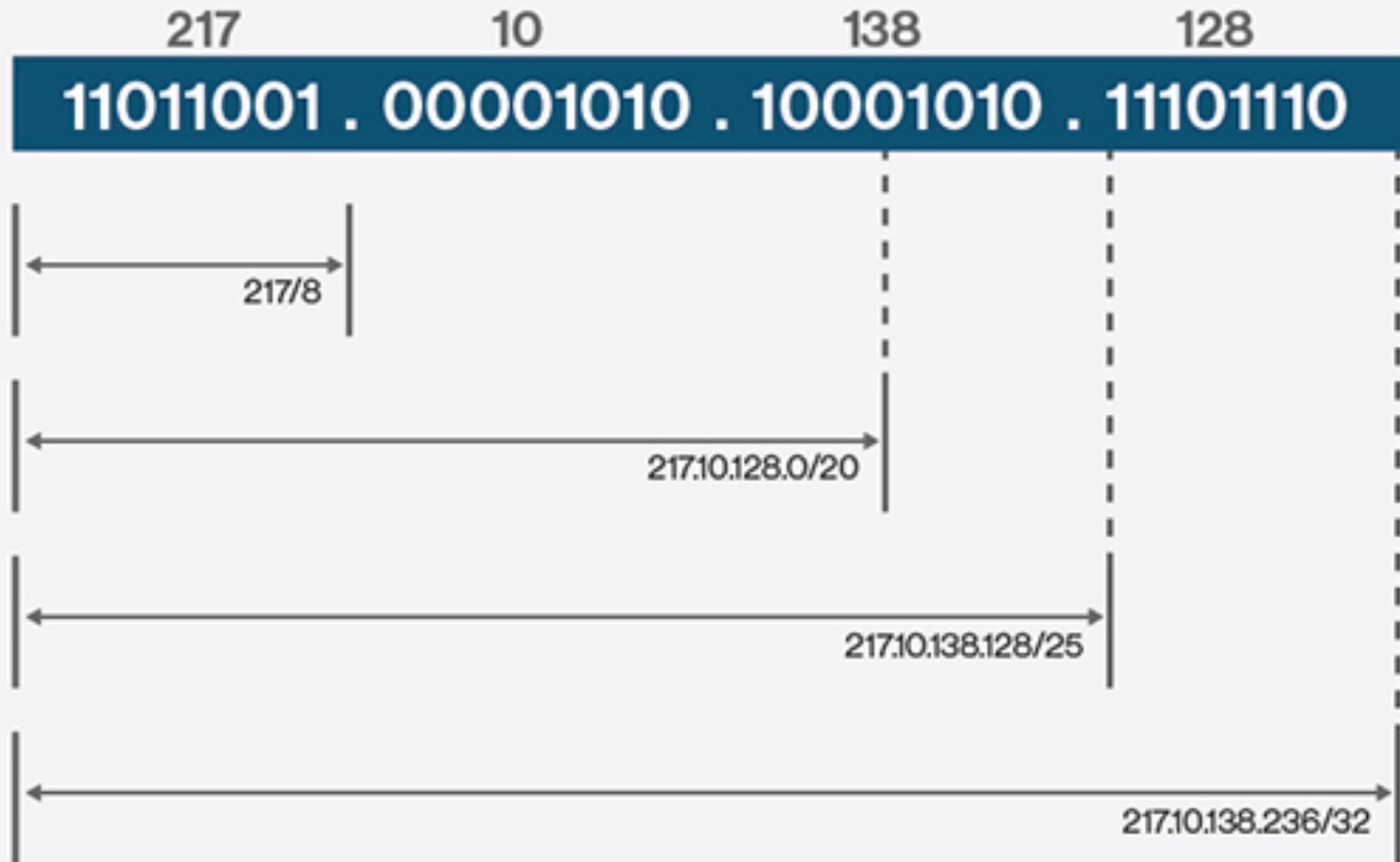
Internet Protocol - IP

Notação de barra (CIDR)



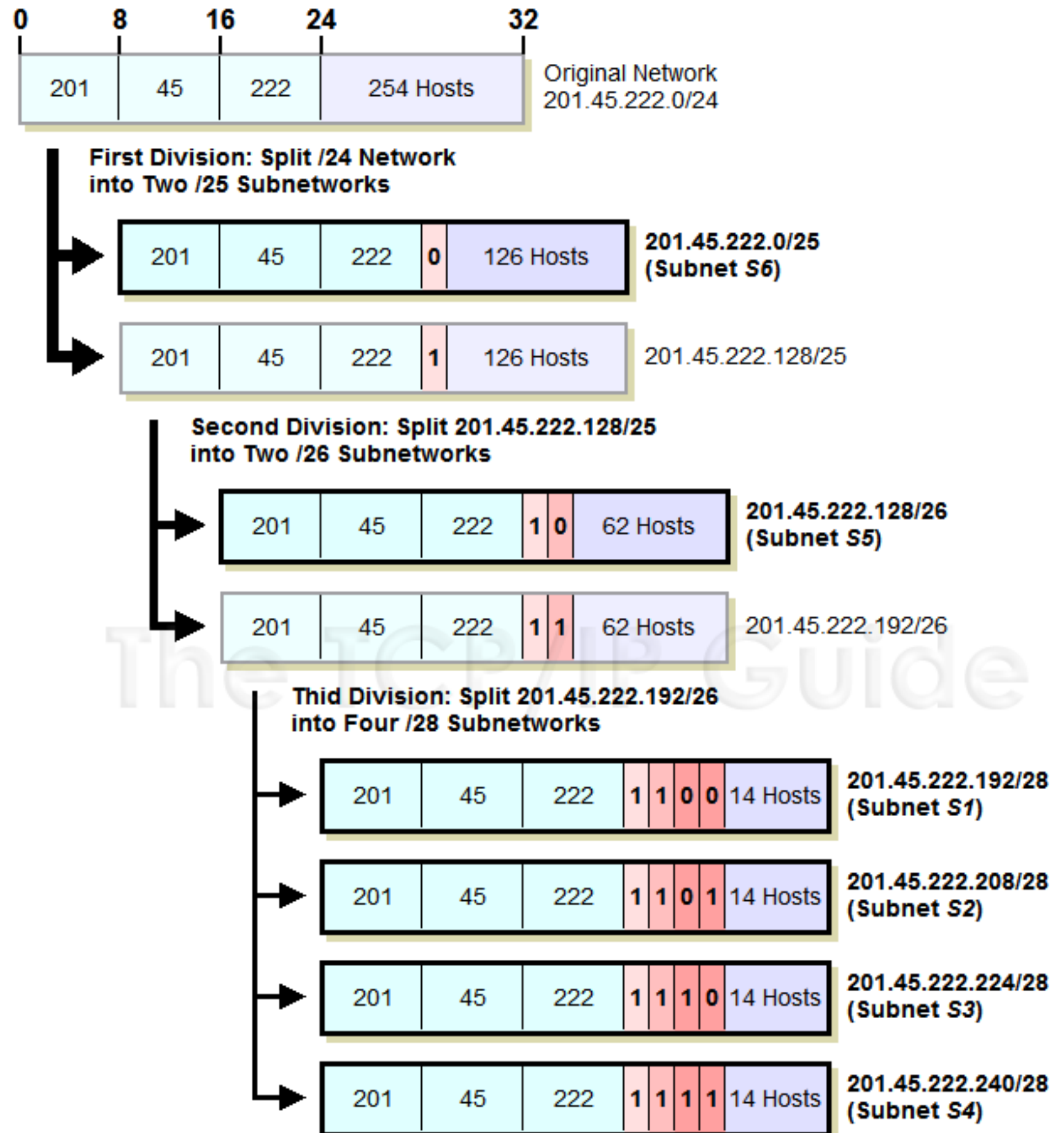
Internet Protocol - IP

Notação de barra (CIDR)



Internet Protocol - IP

CIDR



Internet Protocol - IP

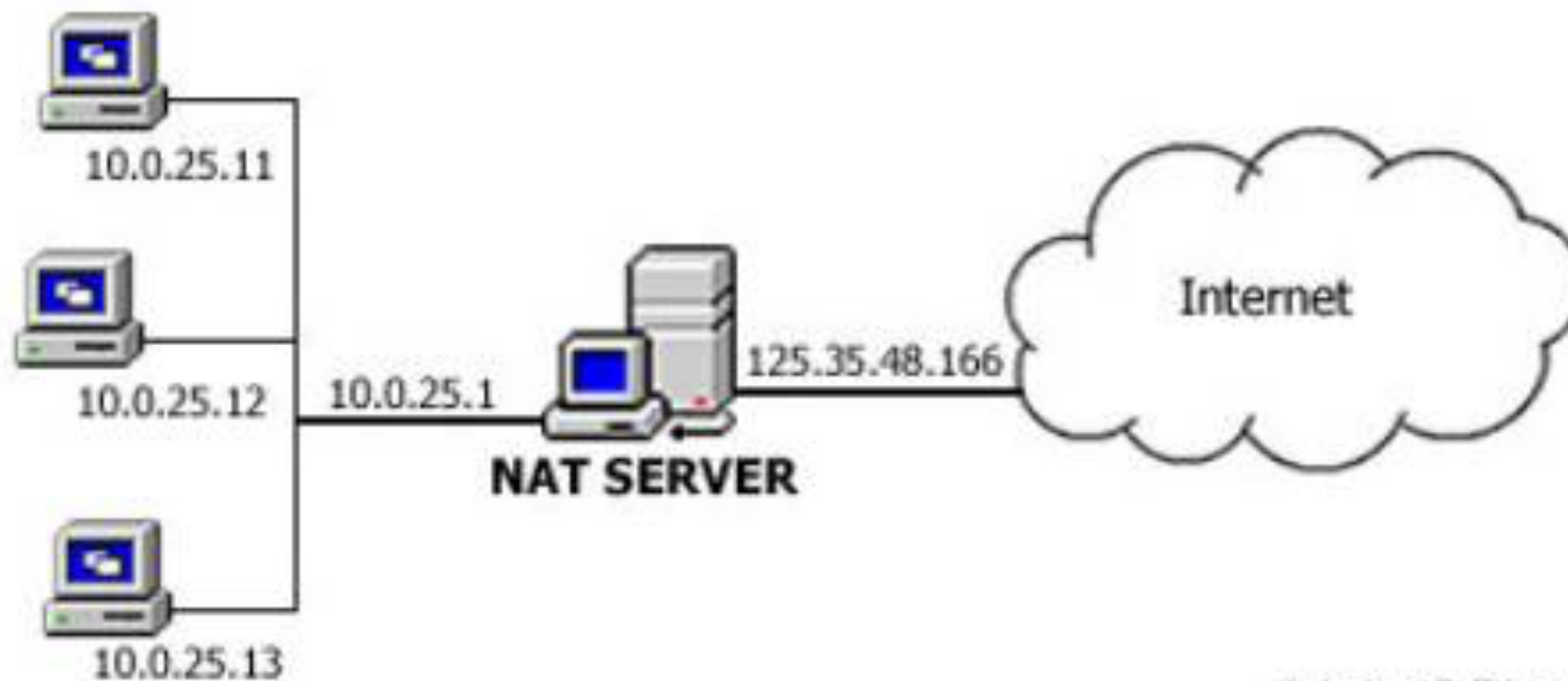
Apesar dessa versão se mostrar muito robusta, de fácil implantação e interoperabilidade, seu projeto original não previu alguns aspectos como:

- O crescimento das redes e um possível esgotamento dos endereços IP;
- O aumento da tabela de roteamento;
- Problemas relacionados a segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

Internet Protocol - IP

NAT - Network Address Translation

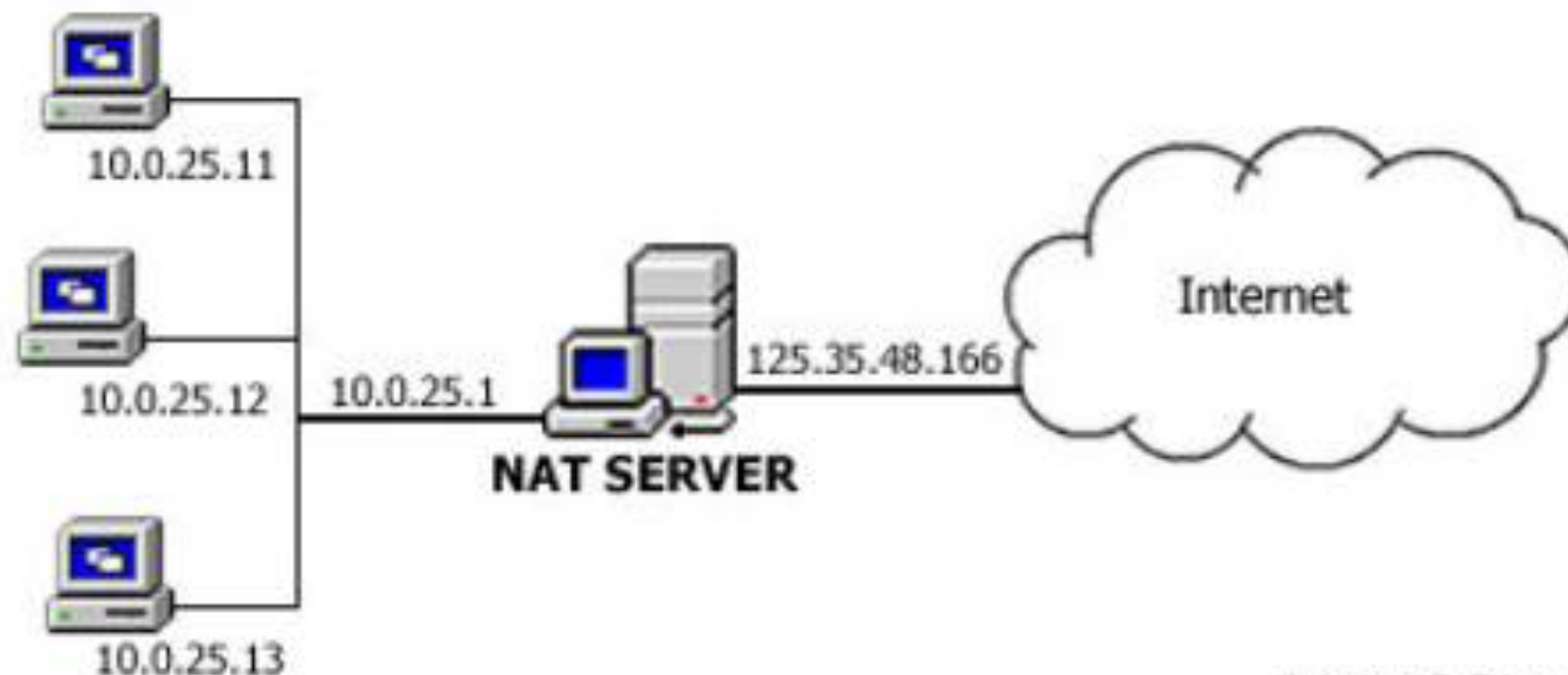
Definida na RFC 3022 (tornou obsoleta a RFC 1631)



Internet Protocol - IP

NAT - Network Address Translation

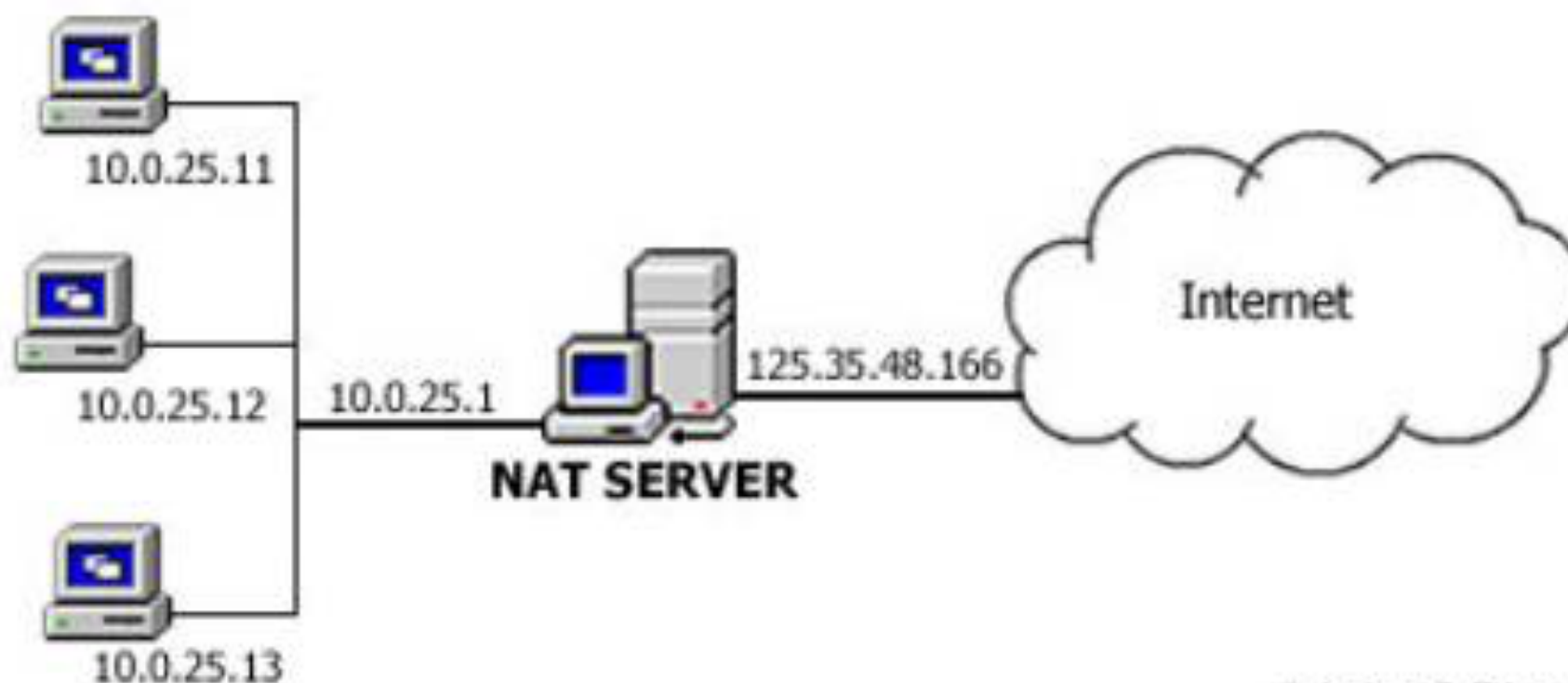
Com o compartilhamento de Internet entre diversas estações numa LAN saindo por um único gateway, surgiu o problema de como os computadores pertencentes à esta LAN poderiam receber as respostas aos seus pedidos feitos para fora da rede.



Internet Protocol - IP

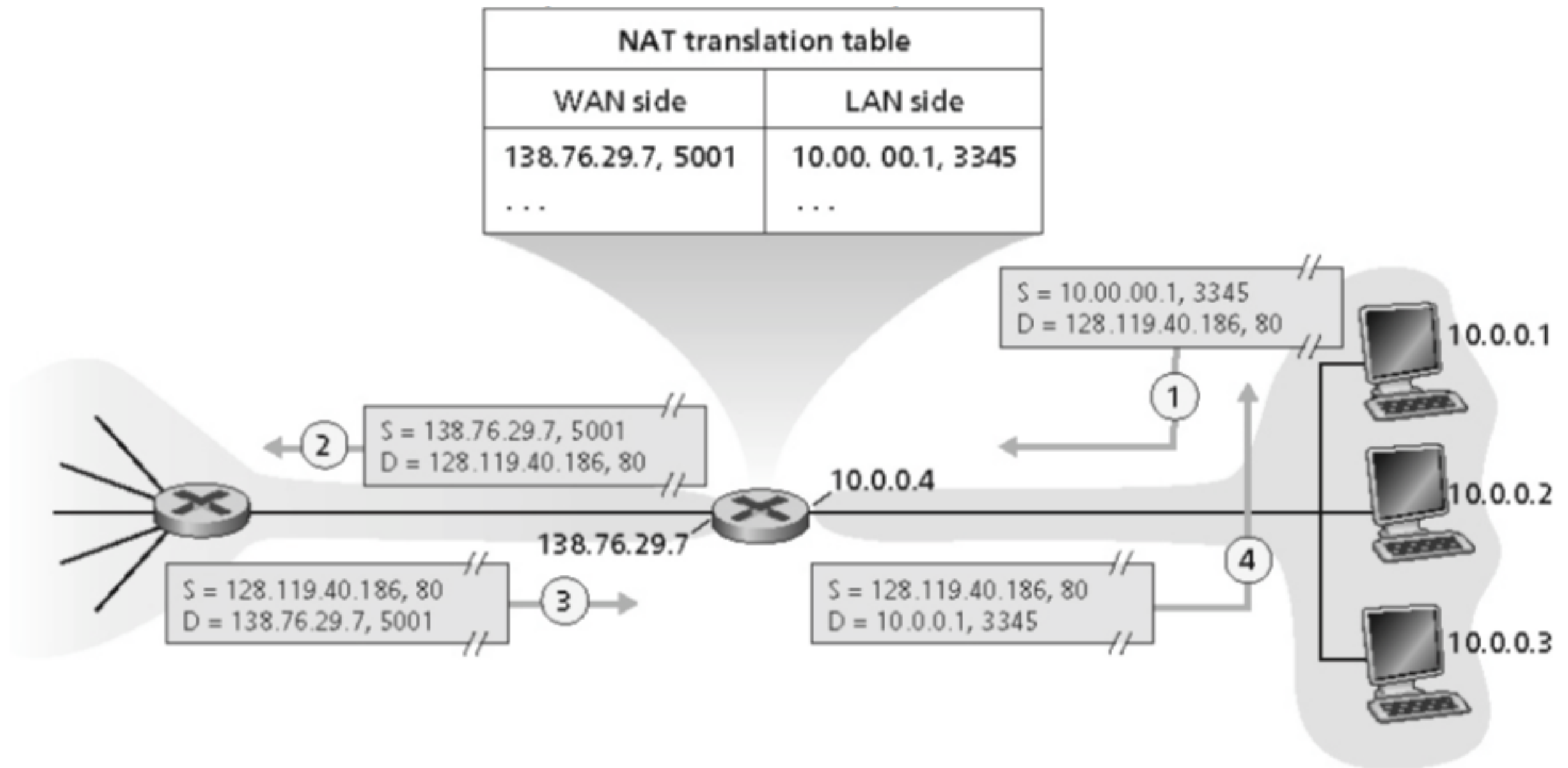
NAT - Network Address Translation

Dentro de uma rede, cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno. No entanto, quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.



Internet Protocol - IP

NAT - Network Address Translation



Internet Protocol - IP

NAT - Network Address Translation

A utilização da NAT mostrou-se eficiente no que diz respeito a economia de endereços IP, além de apresentar alguns outros aspectos positivos, como facilitar a numeração interna das redes, ocultar a topologia das redes e só permitir a entrada de pacotes gerados em resposta a um pedido da rede.

NAT - Network Address Translation

No entanto, o uso da NAT apresenta inconvenientes que não compensam as vantagens oferecidas:

quebra o modelo fim-a-fim da Internet, não permitindo conexões diretas entre dois hosts, o que dificulta o funcionamento de uma série de aplicações, como P2P, VoIP e VPNs.

baixa escalabilidade, pois o número de conexões simultâneas é limitado, além de exigir um grande poder de processamento do dispositivo tradutor.

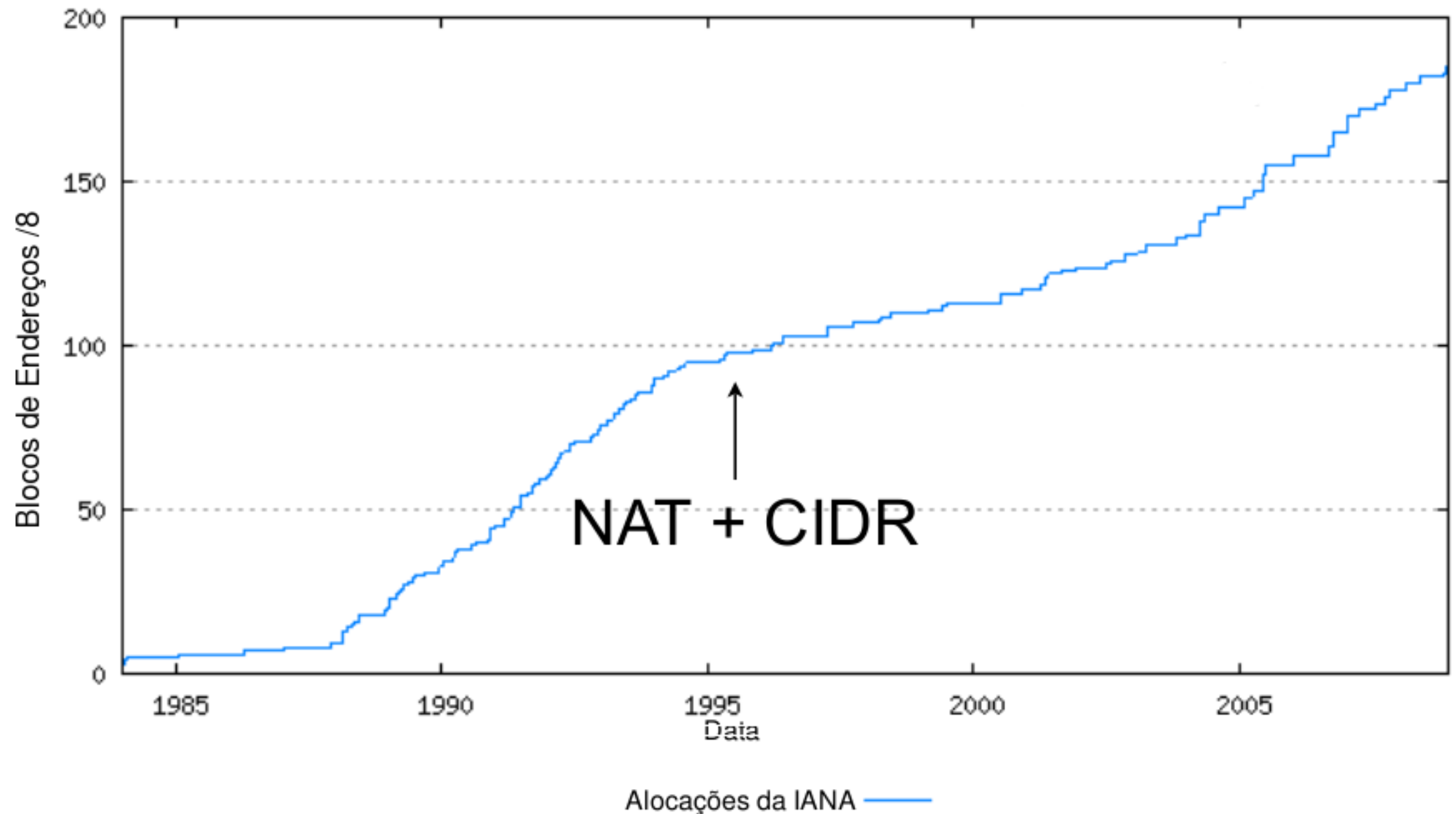
Internet Protocol - IP

NAT - Network Address Translation

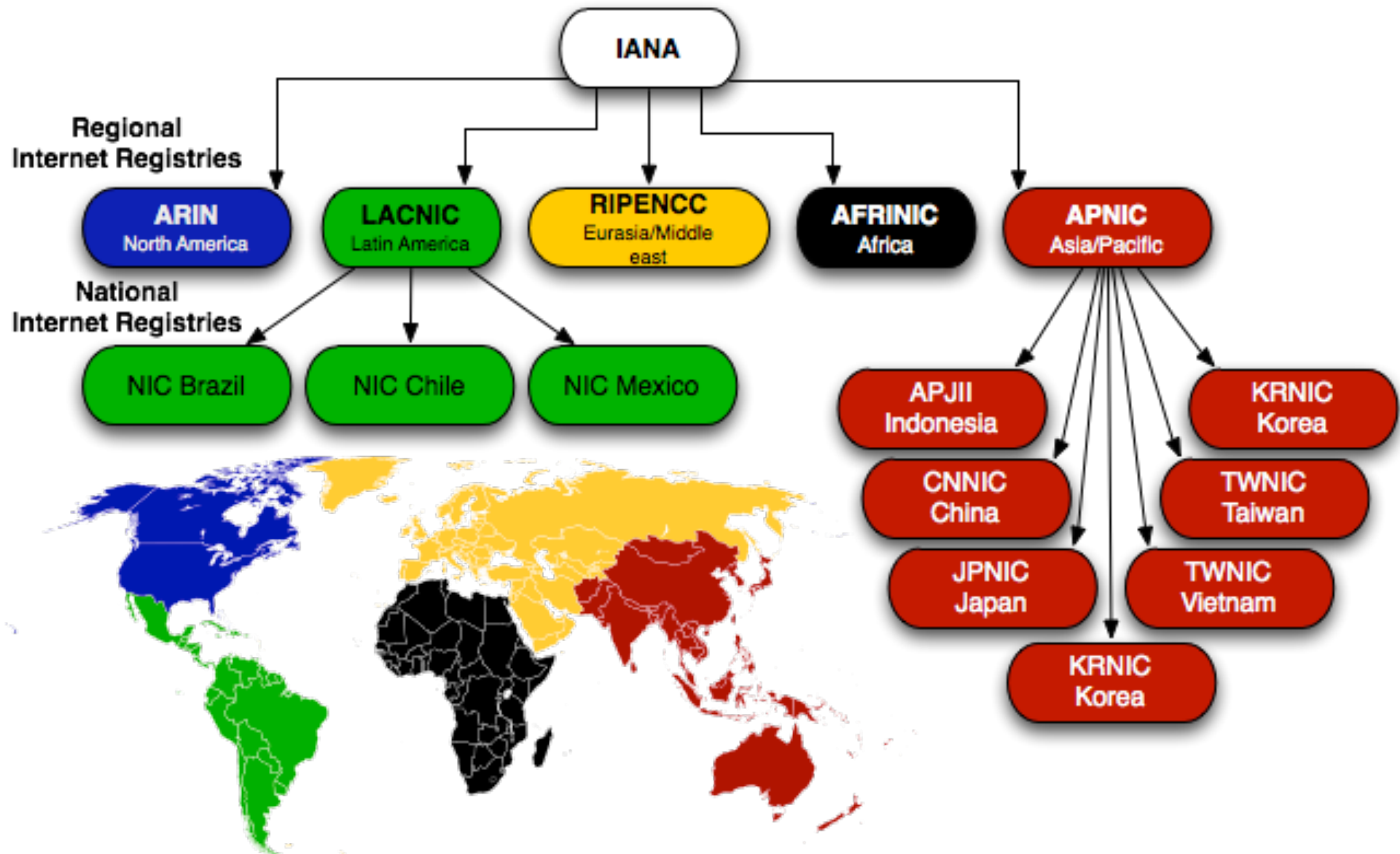
O uso da NAT também **impossibilita rastrear o caminho de pacote**, através de ferramentas como traceroute, por exemplo, e dificulta a utilização de algumas técnicas de segurança como IPSec.

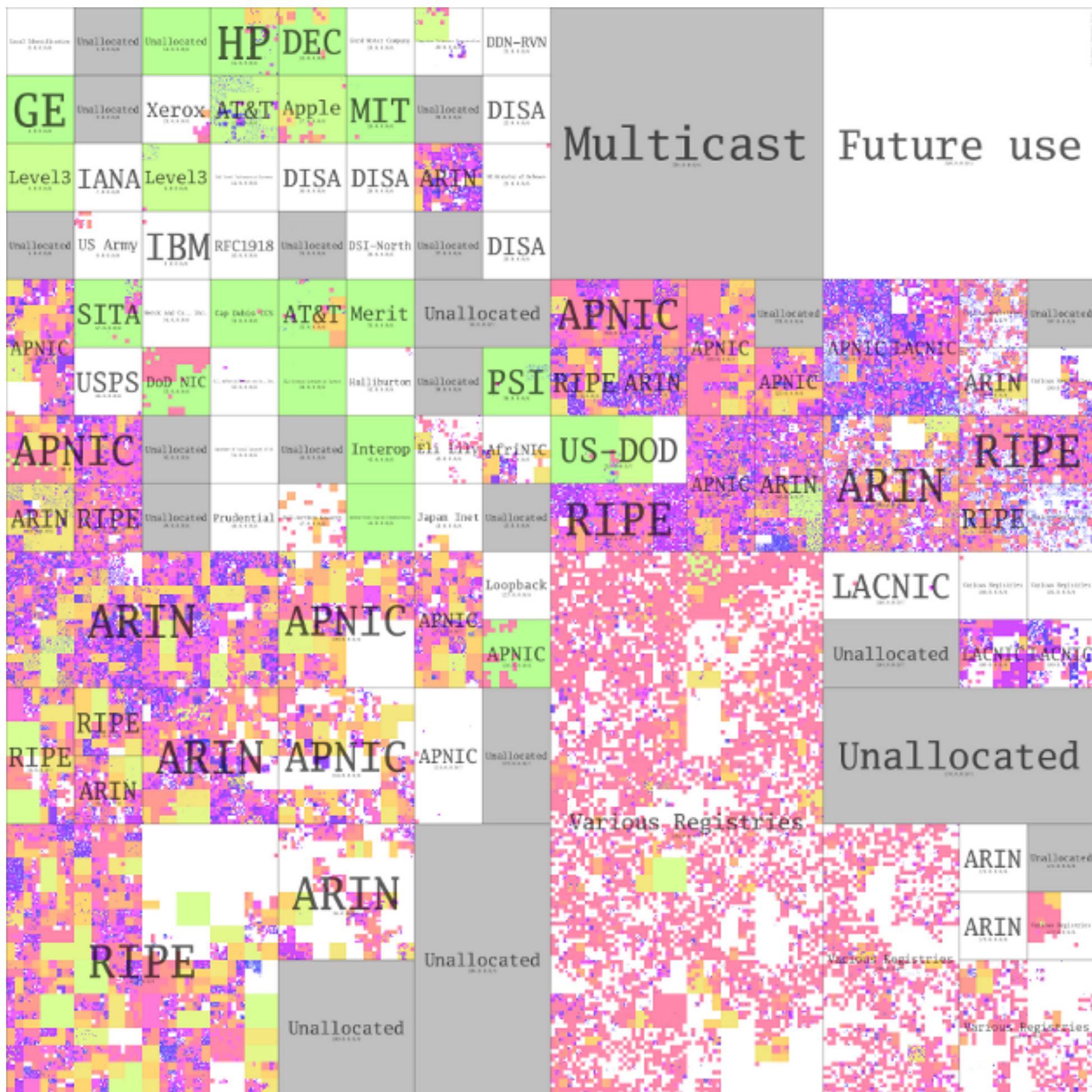
Além disso, seu uso passa uma falsa sensação de segurança, pois, apesar de não permitir a entrada de pacotes não autorizados, a NAT **não realiza nenhum tipo de filtragem ou verificação nos pacotes** que passa por ela.

Internet Protocol - IP



Internet Protocol - IP





Announcement Size



/8
/12
/16
/20
/24
/28
/32

Internet Protocol - IPv6

Embora estas soluções tenham diminuído a demanda por IPs, elas não foram suficientes para resolver os problemas decorrentes do crescimento da Internet. A adoção dessas técnicas reduziu em apenas 14% a quantidade de blocos de endereços solicitados à IANA e a curva de crescimento da Internet continuava apresentando um aumento exponencial.

Internet Protocol - IPv6

Essas medidas, na verdade, serviram para que houvesse mais tempo para se desenvolver uma nova versão do IP, que fosse baseada nos princípios que fizeram o sucesso do IPv4, porém, que fosse capaz de suprir as falhas apresentadas por ele.

Internet Protocol - IPv6

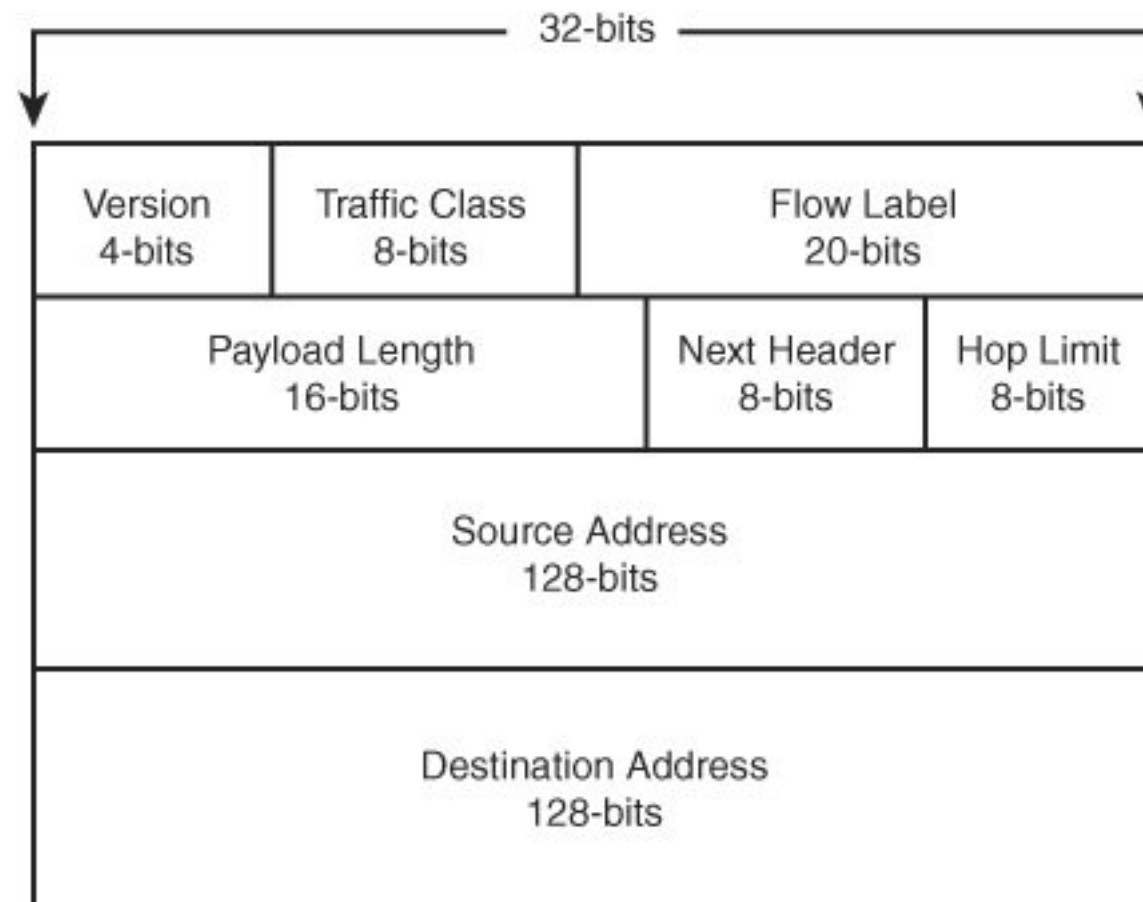
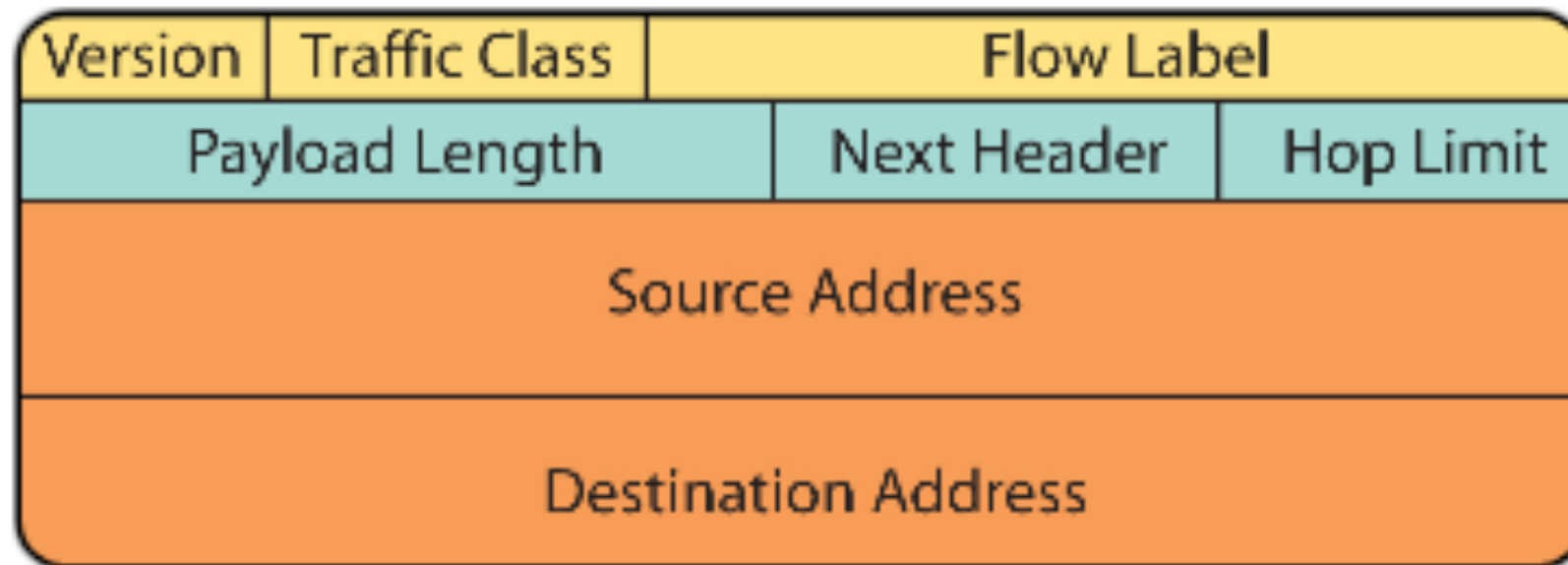
Deste modo, em dezembro de 1993 a IETF formalizou, através da RFC 1550, as pesquisas a respeito da nova versão do protocolo IP, solicitando o envio de projetos e propostas para o novo protocolo.

Umas das primeiras ações do grupo de trabalho da IETF denominado Internet Protocol next generation (IPng).

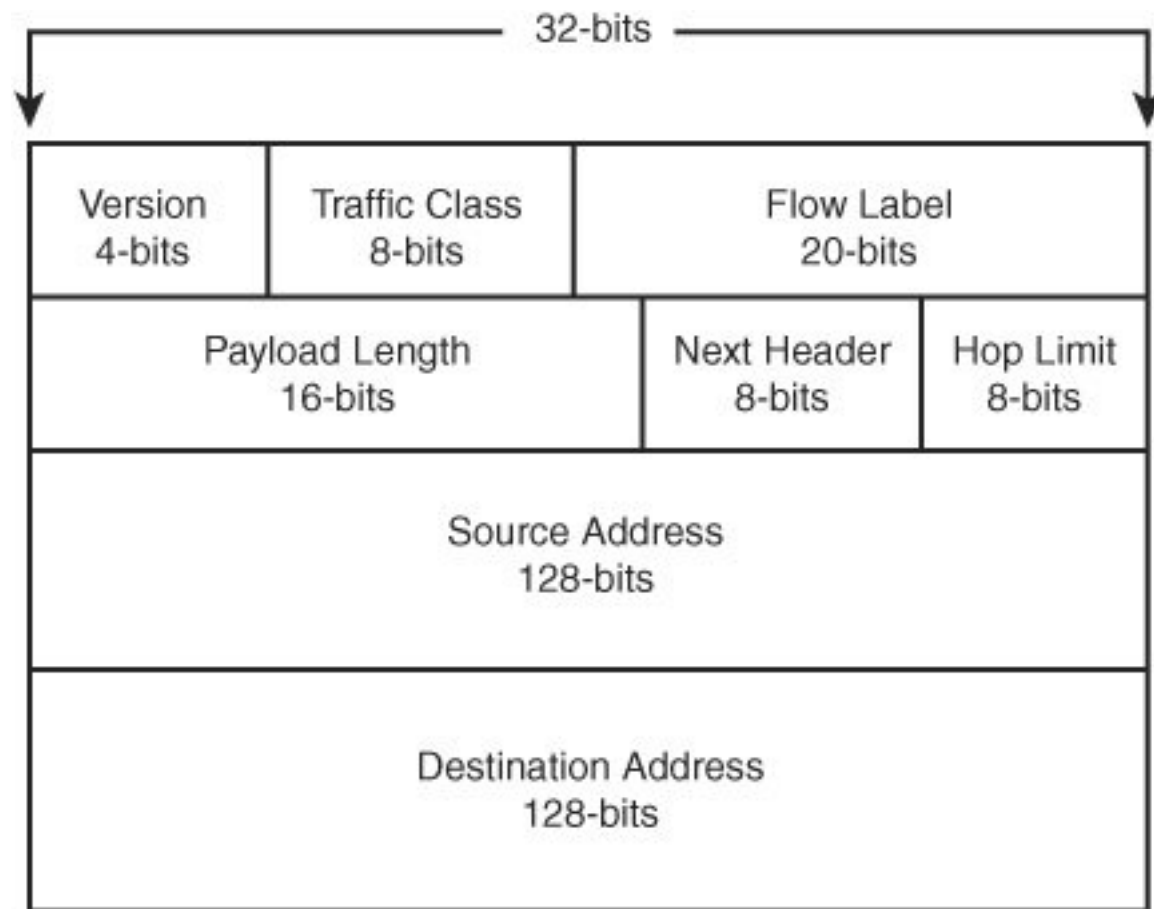
As principais questões:

- **Escalabilidade;**
- **Segurança;**
- **Configuração e administração de rede;**
- **Suporte a QoS;**
- **Mobilidade;**
- **Políticas de roteamento;**
- **Transição.**

Internet Protocol - IPv6



Internet Protocol - IPv6



340.282.366.920.938.463.463.374.607.431.768.211.456

Internet Protocol - IPv6

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

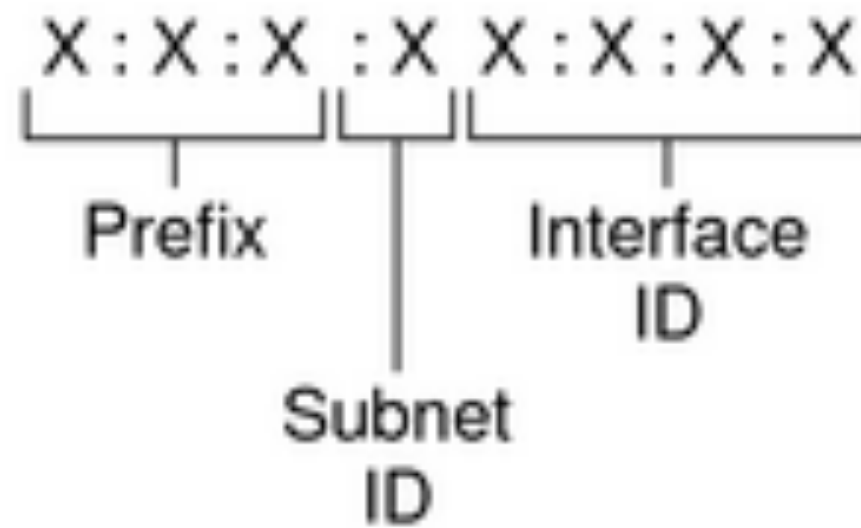
Legend

- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

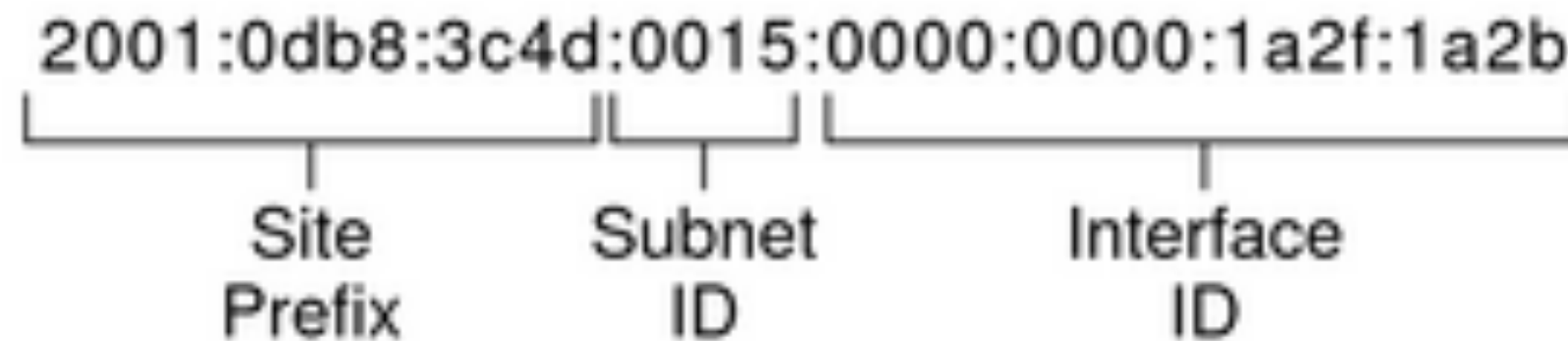
IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
Source Address				
Destination Address				

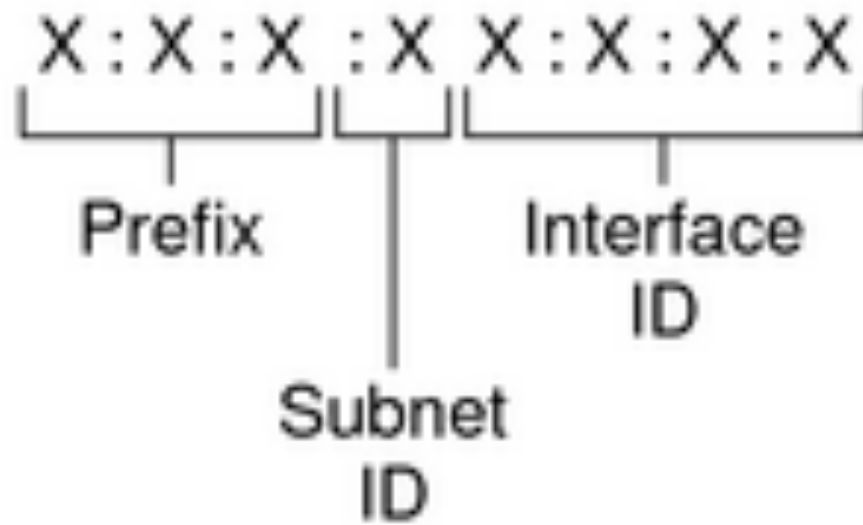
Internet Protocol - IPv6



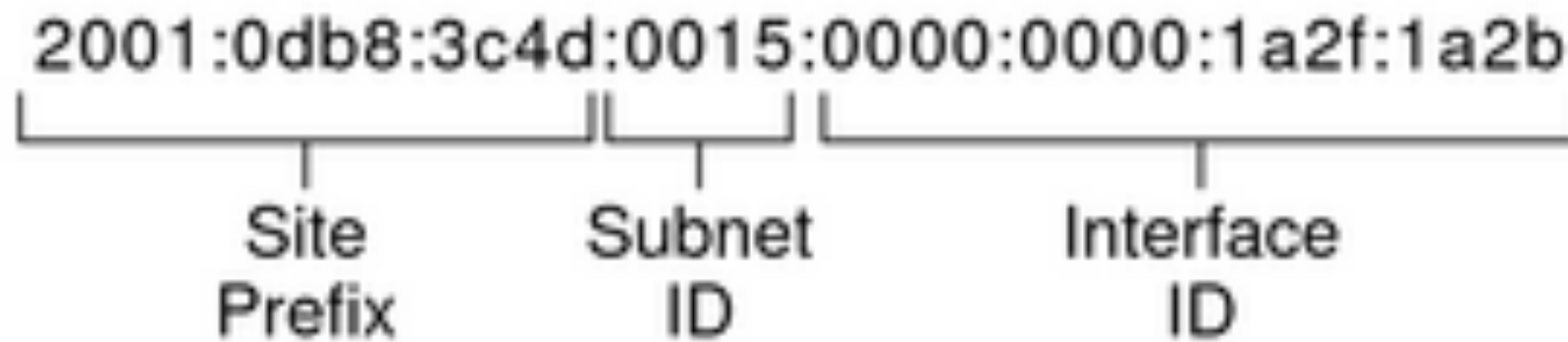
Example:



Internet Protocol - IPv6



Example:



48-bit MAC address

00		0C		42		28		79		45					
00000000		00001100		01000010		00101000		01111001		01000101					
Move manufacturer ID and reverse 7-th bit						Move device ID at the end									
00000010		00001100		01000010		11111111		11111110		00101000		01111001		01000101	
02		0C		42		FF		FE		28		79		45	

64-bit EUI-64 address

Internet Protocol - IPv6



BREAKDOWN OF 128-BIT IPv6 NUMBER

2001:0DB8:0234:AB00:0123:4567:8901:ABCD

2 Global Unicast
Address Indicator

001 Region

0DB8 Local Internet Registry (LIR)
or Internet Service Provider (ISP)

0234 Customer

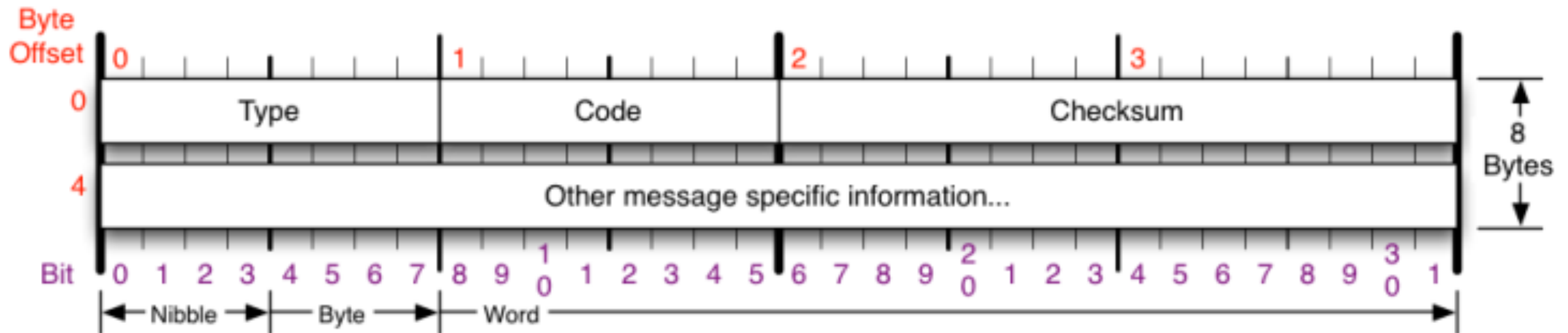
AB00 Subnet

0123:4567:8901:ABCD
The 64-bit Extended Unique Identifier
(EUI-64TM)

Internet Control Message Protocol - ICMP

- **RFC 792**
- ICMP é um protocolo de comunicação de erros para IP
- Quando ocorrem erros de entrega de datagramas, ICMP é usado para relatar esses erros de volta para a origem do datagrama
- O ICMP não corrige o problema de rede encontrado; ela apenas relata o problema.
- ICMP relata sobre o estado do pacote apresentadas apenas para o dispositivo de origem.
- Não propaga informações sobre alterações na rede para roteadores.

Internet Control Message Protocol - ICMP



ICMP Message Types

Checksum

Type Code/Name

- 0 Echo Reply
- 3 Destination Unreachable
 - 0 Net Unreachable
 - 1 Host Unreachable
 - 2 Protocol Unreachable
 - 3 Port Unreachable
 - 4 Fragmentation required, and DF set
 - 5 Source Route Failed
 - 6 Destination Network Unknown
 - 7 Destination Host Unknown
 - 8 Source Host Isolated
 - 9 Network Administratively Prohibited
 - 10 Host Administratively Prohibited
 - 11 Network Unreachable for TOS

Type Code/Name

- 3 Destination Unreachable (continued)
 - 12 Host Unreachable for TOS
 - 13 Communication Administratively Prohibited
- 4 Source Quench
- 5 Redirect
 - 0 Redirect Datagram for the Network
 - 1 Redirect Datagram for the Host
 - 2 Redirect Datagram for the TOS & Network
 - 3 Redirect Datagram for the TOS & Host
- 8 Echo
- 9 Router Advertisement
- 10 Router Selection

Type Code/Name

- 11 Time Exceeded
 - 0 TTL Exceeded
 - 1 Fragment Reassembly Time Exceeded
- 12 Parameter Problem
 - 0 Pointer Problem
 - 1 Missing a Required Operand
 - 2 Bad Length
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply
- 17 Address Mask Request
- 18 Address Mask Reply
- 30 Traceroute

Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Address Resolution Protocol - ARP

Na arquitetura TCP/IP, a função de resolução de endereços é desempenhada pelo protocolo ARP.

O ARP foi originalmente usado em redes Ethernet, mas o seu projeto é genérico, podendo ser usado em outros tipos de tecnologias de rede tais como Token-Ring e FDDI.

Address Resolution Protocol - ARP

O ARP faz o mapeamento dinâmico entre endereços IP de 32 bits e endereços de hardware usados pelas várias tecnologias de enlace.

No caso da tecnologia Ethernet, endereços IP de 32 bits são mapeados em endereços MAC de 48 bits (6 bytes).

O mecanismo de tradução de endereços implementado pelo ARP é baseado no uso de broadcast.

Address Resolution Protocol - ARP

Cache ARP

Para manter o número de broadcasts a um nível mínimo, os hosts que usam o ARP mantêm um cache de mapeamentos Internet-Ethernet já resolvidos pois, assim, não precisam usar o ARP toda hora que se quiser transmitir um pacote.

Antes de transmitir um pacote o host sempre examina o seu cache ARP, buscando verificar se já existe mapeamento anterior para o endereço destino

Address Resolution Protocol - ARP

Cache ARP

Para que o cache não cresça demasiadamente, entradas são removidas se não forem usadas dentro de um certo período de tempo.

O cache ARP também é chamado de Tabela ARP.

Address Resolution Protocol - ARP

Cache ARP

Tráfego adicional na rede é evitado fazendo o emissor do ARP Request incluir o seu próprio mapeamento Internet-Ethernet na primitiva. Isso é feito para que o host destino possa adicionar esse mapeamento no seu cache.

Como o ARP Request inicial é uma mensagem do tipo broadcast, todos os computadores da rede vão recebê-lo, e serão capazes de aprender esse mapeamento e armazená-lo nos seus respectivos cache.

Address Resolution Protocol - ARP

