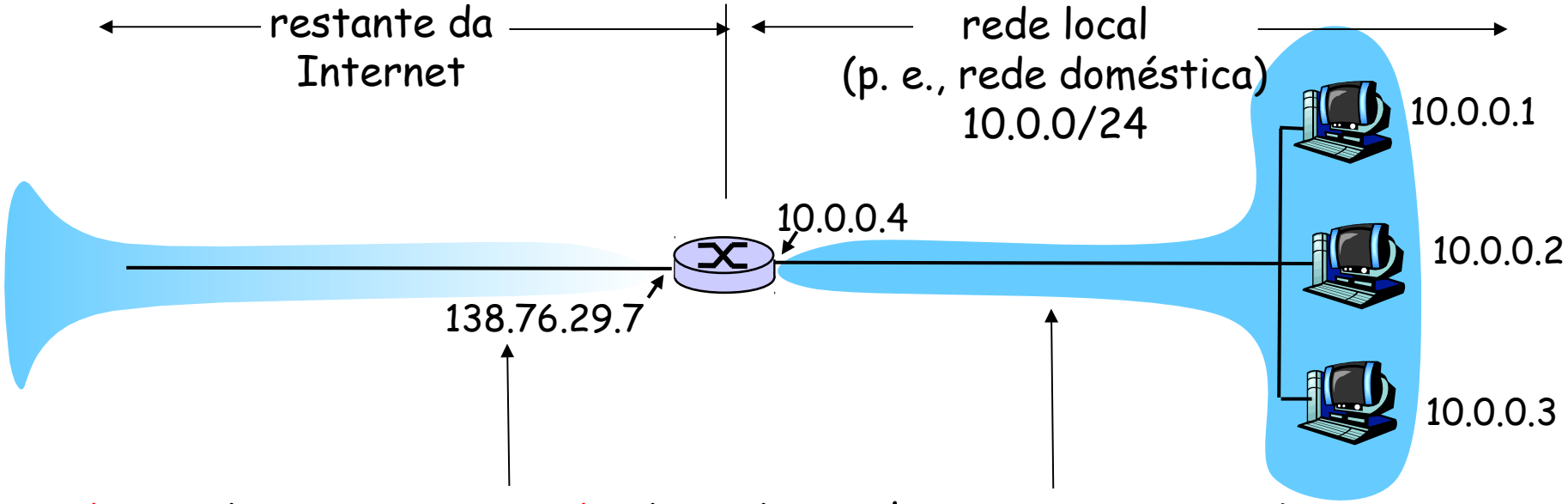
Capítulo 4: Camada de rede

Objetivos do capítulo:

- entender os princípios por trás dos serviços da camada de rede:
  - modelos de serviço da camada de rede
  - repasse *versus* roteamento
  - como funciona um roteador
  - roteamento (seleção de caminho)
  - lidando com escala
  - tópicos avançados: IPv6, mobilidade
- instanciação, implementação na Internet

NAT: Network Address Translation



todos os datagramas *saindo* da rede local têm mesmo endereço IP NAT de origem: 138.76.29.7, mas diferentes números de porta de origem

datagramas com origem ou destino nesta rede têm endereço 10.0.0/24 para origem/destino (como sempre)

NAT: Network Address Translation

- motivação: rede local usa apenas um endereço IP no que se refere ao mundo exterior:
  - intervalo de endereços não necessário pelo ISP: apenas um endereço IP para todos os dispositivos
  - pode mudar os endereços dos dispositivos na rede local sem notificar o mundo exterior
  - pode mudar de ISP sem alterar os endereços dos dispositivos na rede local
  - dispositivos dentro da rede local não precisam ser explicitamente endereçáveis ou visíveis pelo mundo exterior (uma questão de segurança).

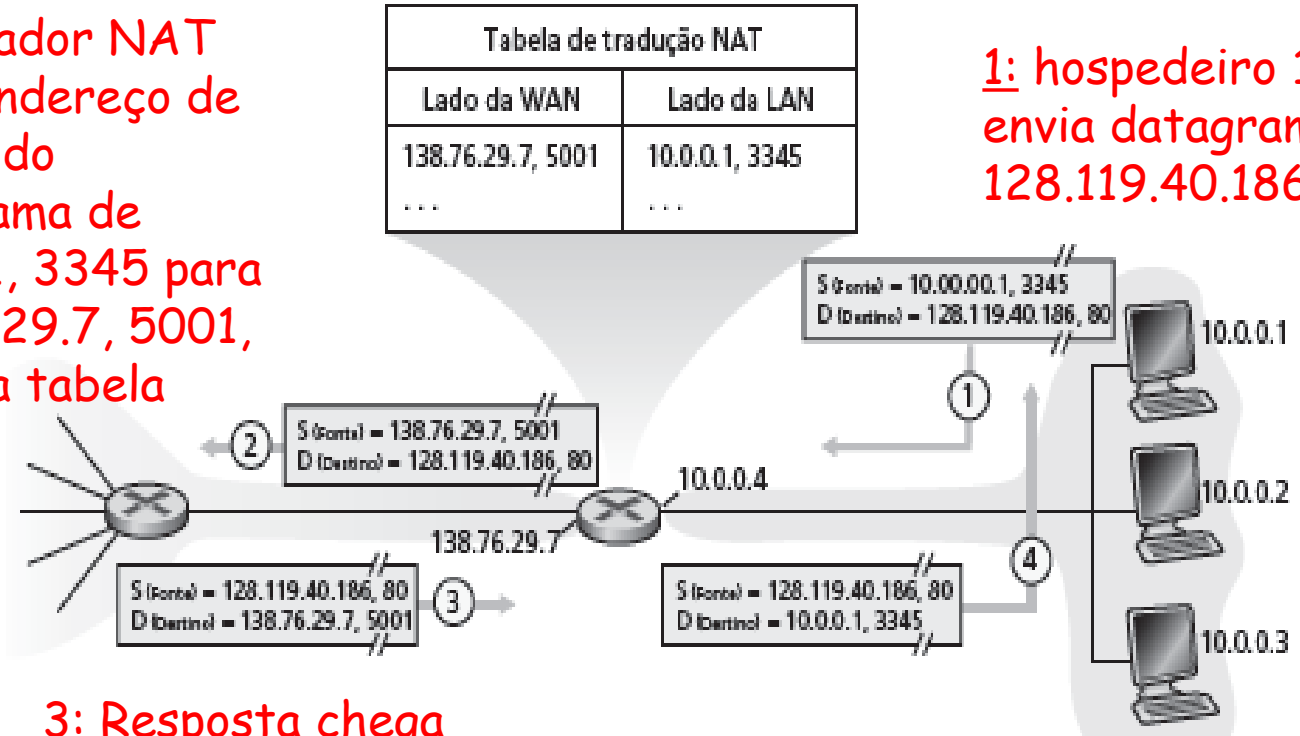
Implementação: roteador NAT deve:

- *enviando datagramas: substituir* (endereço IP de origem, # porta) de cada datagrama saindo por (endereço IP da NAT, novo # porta)
  - . . . clientes/servidores remotos responderão usando (endereço IP da NAT, novo # porta) como endereço de destino

- *lembrar (na tabela de tradução NAT)* de cada par de tradução (endereço IP de origem, # porta) para (endereço IP da NAT, novo # porta)

- *recebendo datagramas: substituir* (endereço IP da NAT, novo # porta) nos campos de destino de cada datagrama chegando por (endereço IP origem, # porta) correspondente, armazenado na tabela NAT

2: roteador NAT muda endereço de origem do datagrama de 10.0.0.1, 3345 para 138.76.29.7, 5001, atualiza tabela



1: hospedeiro 10.0.0.1 envia datagrama para 128.119.40.186, 80

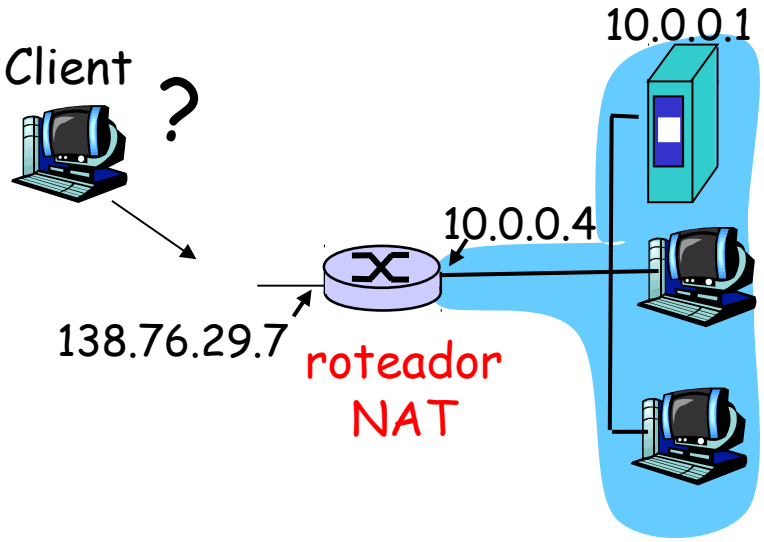
3: Resposta chega endereço destino: 138.76.29.7, 5001

4: roteador NAT muda endereço de destino do datagrama de 138.76.29.7, 5001 para 10.0.0.1, 3345

- campo de número de porta de 16 bits:
  - 60.000 conexões simultâneas com um único endereço no lado da LAN!
- NAT é controverso:
  - roteadores só devem processar até a camada 3
  - viola argumento de fim a fim
    - a possibilidade de NAT deve ser levada em conta pelos projetistas da aplicação, p. e., aplicações P2P
  - a falta de endereços deverá ser resolvida pelo IPv6

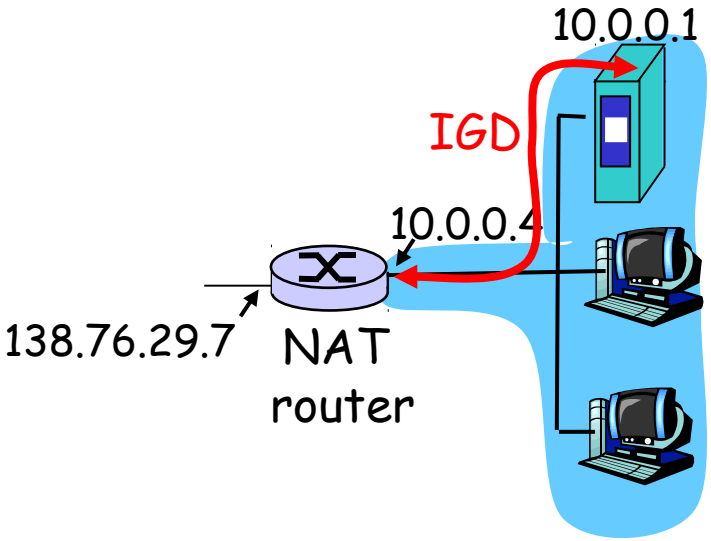
Problema da travessia da NAT

- cliente quer se conectar ao servidor com endereço 10.0.0.1
  - endereço do servidor 10.0.0.1 local à LAN (cliente não pode usá-lo como endereço destino)
  - apenas um endereço NAT visível externamente: 138.76.29.7
- solução 1: configure a NAT estaticamente para repassar as solicitações de conexão que chegam a determinada porta ao servidor
  - p. e., (138.76.29.7, porta 80) sempre repassado para 10.0.0.1 porta 25000

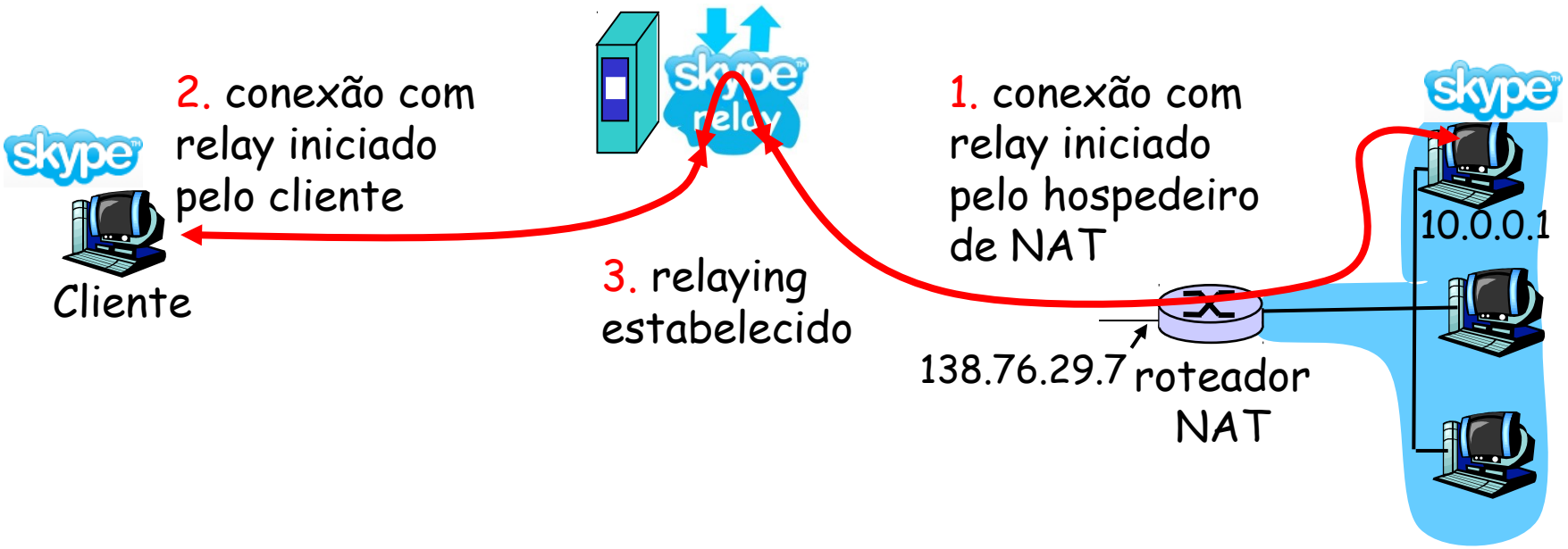


- solução 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Permite que o hospedeiro com NAT:
  - descubra endereço IP público (138.76.29.7)
  - inclua/remova mapeamentos de porta (com tempos de posse)

ou seja, automatizar configuração estática do mapa de porta NAT

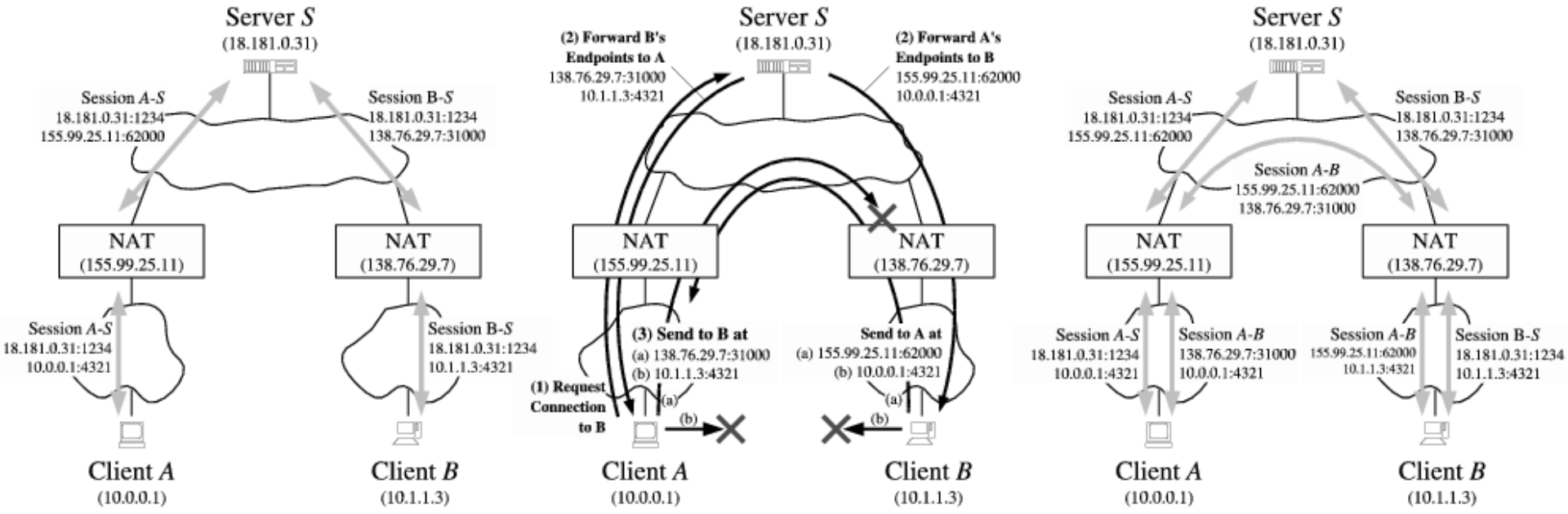


- solução 3: repasse (usado no Skype)
  - cliente com NAT estabelece conexão com repasse
  - cliente externo se conecta ao repasse
  - repasse liga pacotes entre duas conexões



- solução 4: Hole Punching
  - Tipos de NAT
    - full cone: mapeamento um para um (**OK**)
      - iAddr:iPort ↔ eAddr:ePort
      - qualquer hospedeiro destino
    - (addres- ou port-) restricted cone (**OK**)
      - iAddr:iPort ↔ eAddr:ePort
      - hospedeiro destino para quem foi enviado pacotes
    - Simétrico (**Impossível**)
      - iAddr:iPort ↔ eAddr:ePort1 ↔ dAddr1:dPort1
      - iAddr:iPort ↔ eAddr:ePort2 ↔ dAddr1:dPort2

- Hole Punching em UDP
  - A perguntar para S como alcançar B
  - S envia endereço de B para A e de A para B
  - A e B iniciam envio de datagramas UDP

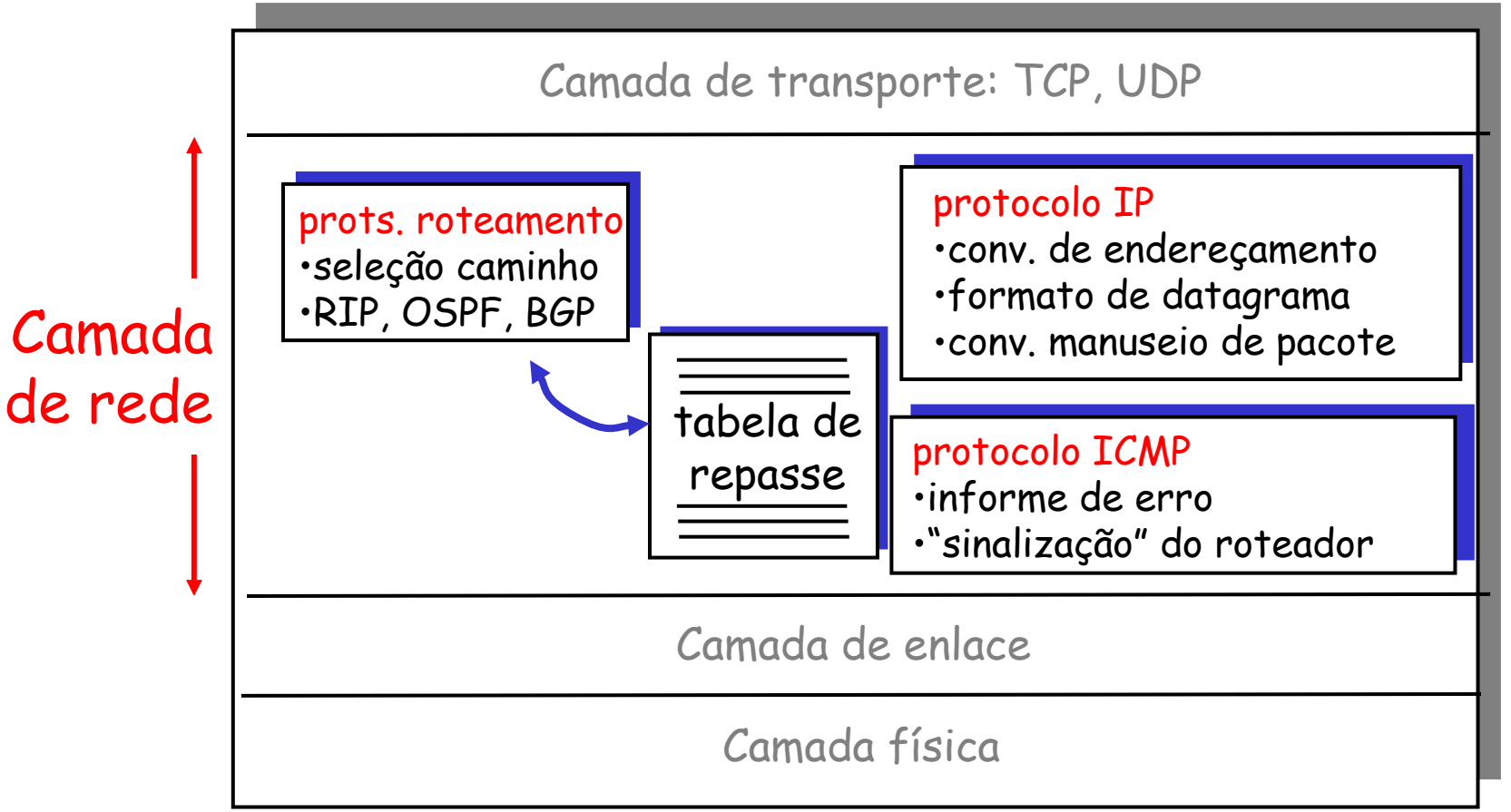


Capítulo 4: Camada de rede

- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- 4.3 O que há dentro de um roteador?
- 4.4 IP: Internet Protocol
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- 4.5 Algoritmos de roteamento
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico
- 4.6 Roteamento na Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Roteamento broadcast e multicast

A camada de rede da Internet

Funções na camada de rede do hospedeiro e roteador:



ICMP: Internet Control Message Protocol

- usado por hospedeiros & roteadores para comunicar informações em nível de rede
  - relato de erro: hospedeiro, rede, porta, protocolo inalcançável
  - eco de solicitação/ resposta (usado por ping)
- camada de rede "acima" do IP:
  - msgs ICMP transportadas em datagramas IP
- mensagem ICMP: tipo, código mais primeiros 8 bytes do datagrama IP causando erro

Tipo	Cód,	Descrição
0	0	resposta de eco (ping)
3	0	rede de destino inalcançável
3	1	hosp. de destino inalcançável
3	2	protocolo de destino inalcançável
3	3	porta de destino inalcançável
3	6	rede de destino desconhecida
3	7	hosp. de destino desconhecido
4	0	redução da fonte (controle de congestionamento – não usado)
8	0	solicitação de eco (ping)
9	0	anúncio de roteador
10	0	descoberta do roteador
11	0	TTL expirado
12	0	cabeçalho IP inválido

Traceroute e ICMP

- origem envia série de segmentos UDP ao destino
  - primeiro tem TTL = 1
  - segundo tem TTL = 2 etc.
  - número de porta improvável
- quando nº datagrama chegar no nº roteador:
  - roteador descarta datagrama
  - e envia à origem uma msg ICMP (tipo 11, código 0)
  - mensagem inclui nome do roteador & endereço IP

- quando a mensagem ICMP chega, origem calcula RTT
- traceroute faz isso 3 vezes

Critério de término

- segmento UDP por fim chega no hospedeiro de destino
- destino retorna pacote ICMP "host inalcançável" (tipo 3, código 3)
- quando origem recebe esse ICMP, termina.

Capítulo 4: Camada de rede

- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- 4.3 O que há dentro de um roteador?
- 4.4 IP: Internet Protocol
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- 4.5 Algoritmos de roteamento
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico
- 4.6 Roteamento na Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Roteamento broadcast e multicast

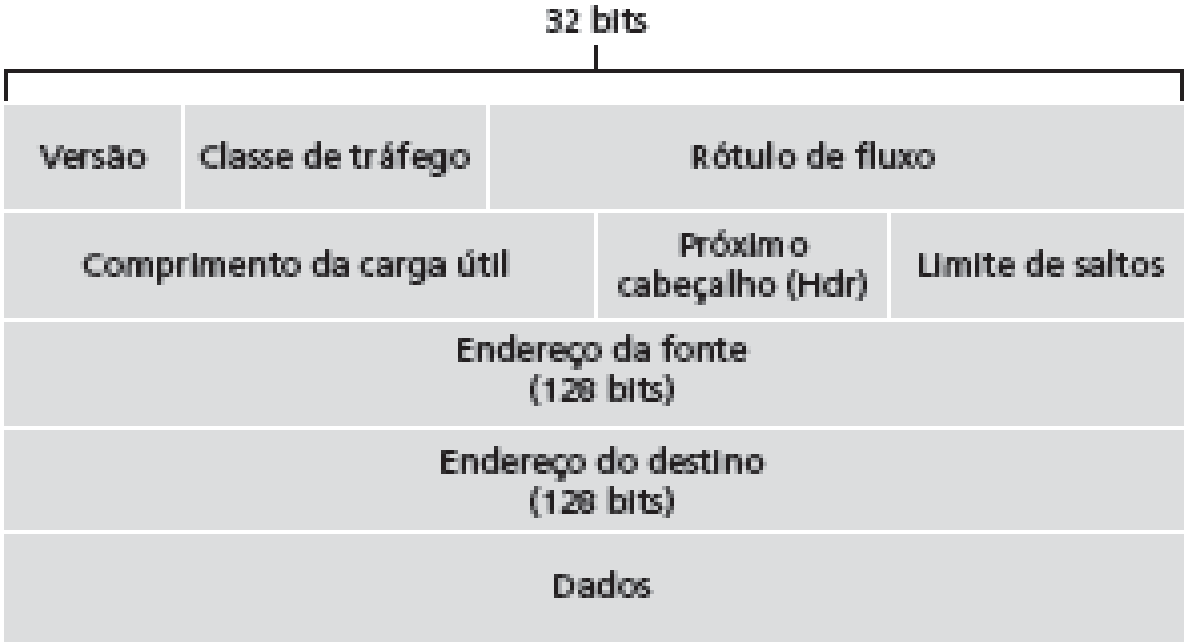
IPv6

- motivação inicial: espaço de endereço de 32 bit já está completamente alocado
- motivação adicional:
  - formato de cabeçalho ajuda a agilizar processamento e repasse
  - mudanças para facilitar QoS

  formato de datagrama IPv6:
  - cabeçalho de 40 bytes de tamanho fixo
  - fragmentação não permitida
  - endereço MAC faz parte do IP

Cabeçalho IPv6

classe de tráfego: identificar prioridade entre datagramas no fluxo
rótulo de fluxo: identificar datagramas no mesmo "fluxo."
próximo cabeçalho: identificar protocolo da camada superior para dados



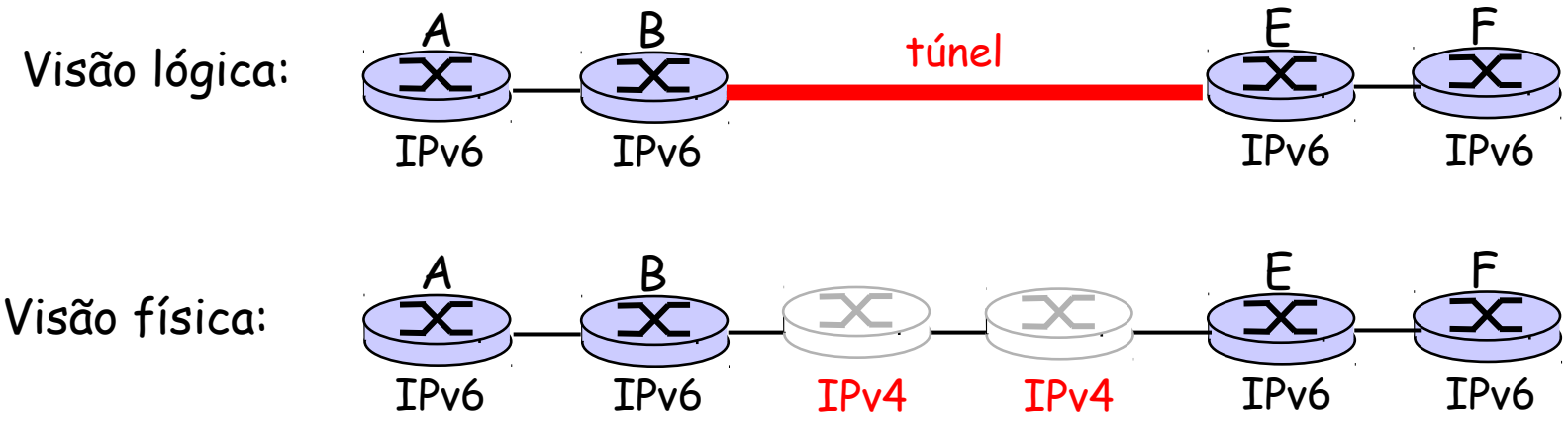
Outras mudanças do IPv4

- *soma de verificação*: removida inteiramente para reduzir tempo de processamento em cada salto
- *opções:* permitidas, mas fora do cabeçalho, indicadas pelo campo de "Próximo Cabeçalho"
- *ICMPv6:* nova versão do ICMP
  - tipos de mensagem adicionais, p. e. "Pacote Muito Grande"
  - funções de gerenciamento de grupo multicast

Transição de IPv4 para IPv6

- nem todos os roteadores podem ser atualizados simultaneamente
  - sem "dia de conversão"
  - como a rede operará com roteadores IPv4 e IPv6 misturados?
- *implantação de túnel:* IPv6 transportado como carga útil no datagrama IPv4 entre roteadores IPv4

Implantação de túnel



Visão lógica:

Visão física: