Camada de enlace

REDES DE COMPUTADORES E A INTERNET 5ª edição
Uma Abordagem Top-Down

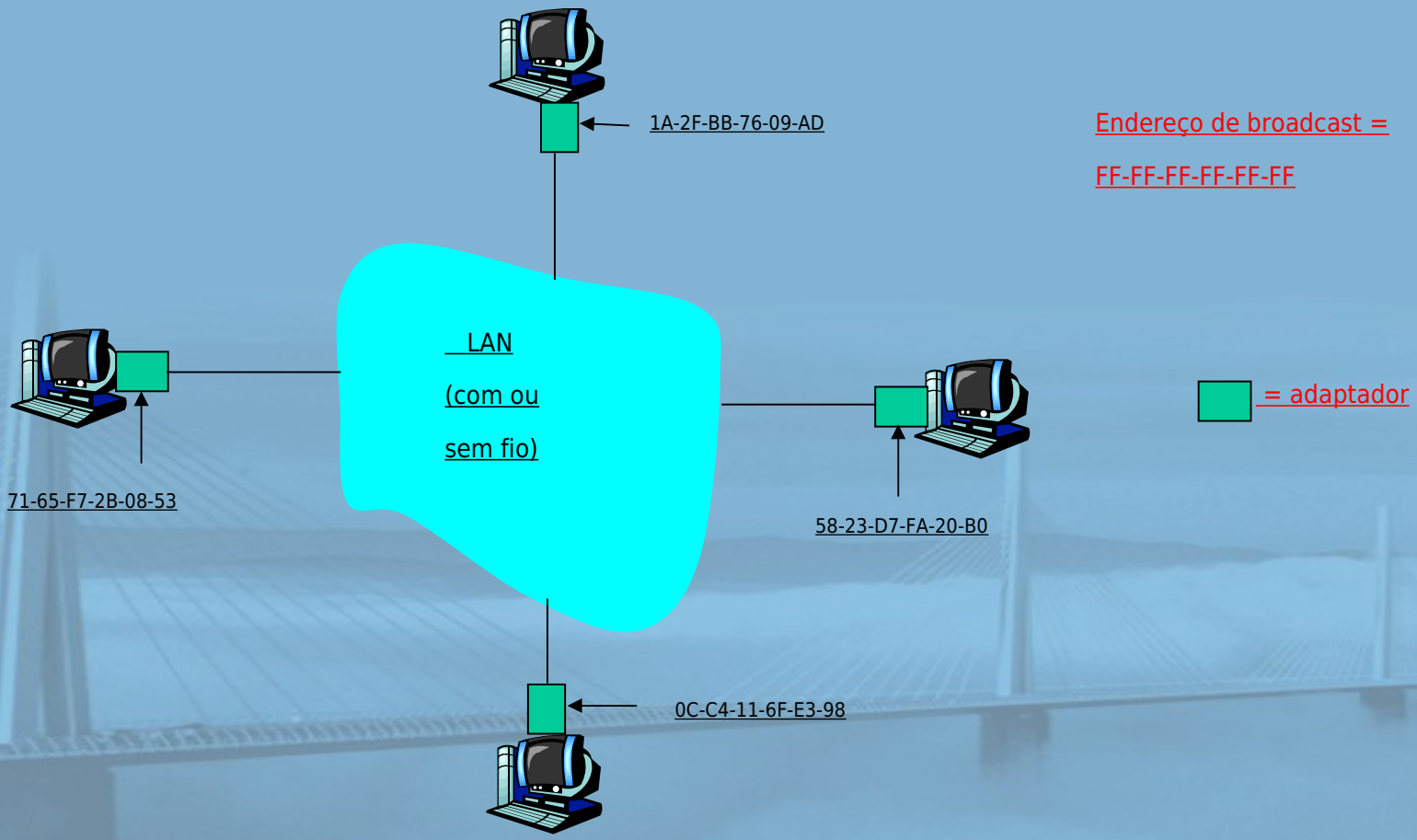
- 5.1 Introdução e serviços
- 5.2 Detecção e correção de erros
- 5.3 Protocolos de acesso múltiplo
- 5.4 Endereçamento na camada de enlace
- 5.5 Ethernet
- 5.6 Comutadores de camada de enlace
- 5.7 PPP
- 5.8 Virtualização de enlace: MPLS
- 5.9 Um dia na vida de uma solicitação de página Web

Endereçamento MAC e ARP

- Endereço IP de 32 bits:
  - endereço da *camada de rede*
  - usado para levar datagrama até sub-rede IP de destino
- Endereço MAC (ou LAN ou físico ou Ethernet) :
  - função: *levar quadro de uma interface para outra interface conectada fisicamente (na mesma rede)*
  - Endereço MAC de 48 bits (para maioria das LANs)
    - queimado na ROM da NIC, às vezes também configurável por software

Endereços de LAN e ARP

Cada adaptador na LAN tem endereço de LAN exclusivo



Endereço de broadcast =
FF-FF-FF-FF-FF-FF

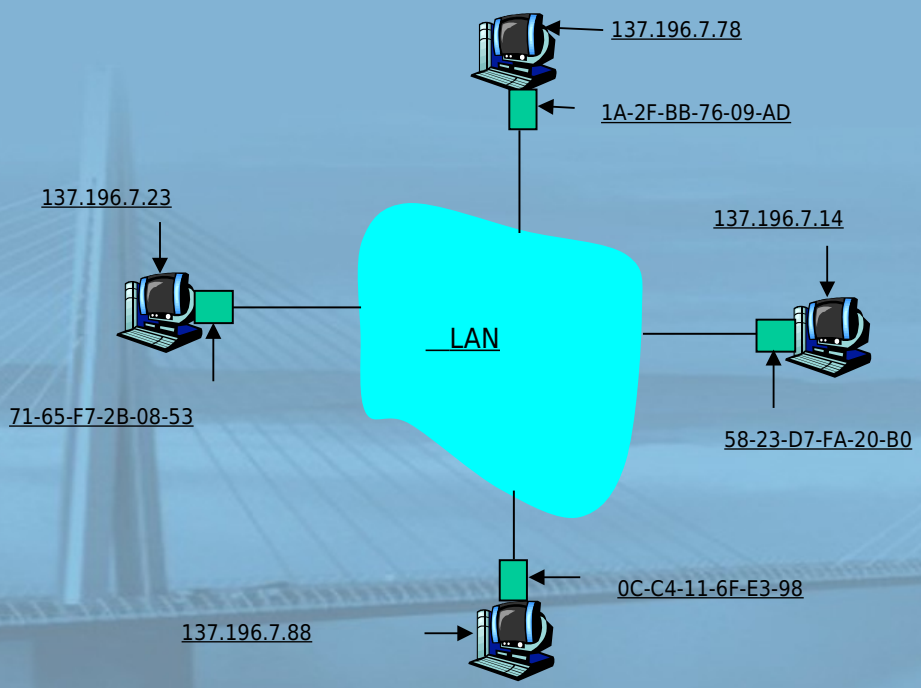
= adaptador

Endereços de LAN (mais)

- alocação de endereço MAC administrada pelo IEEE
- fabricante compra parte do espaço de endereços MAC (para garantir exclusividade)
- analogia:
  - (a) Endereço MAC: como o CPF
  - (b) Endereço IP: como o endereço postal
- endereço MAC plano → portabilidade
  - pode mover placa de LAN de uma LAN para outra
- endereço IP hierárquico NÃO portável
  - endereço depende da sub-rede IP à qual o nó está conectado

ARP: Address Resolution Protocol

Pergunta: Como determinar endereço MAC de B sabendo o endereço IP de B?



- Cada nó IP (hosp., roteador) na LAN tem tabela ARP
- Tabela ARP: mapeamentos de endereço IP/MAC para alguns nós da LAN

<endereço IP; endereço MAC; TTL>

  - TTL (Time To Live): tempo após o qual o mapeamento de endereço será esquecido (normalmente, 20 min)

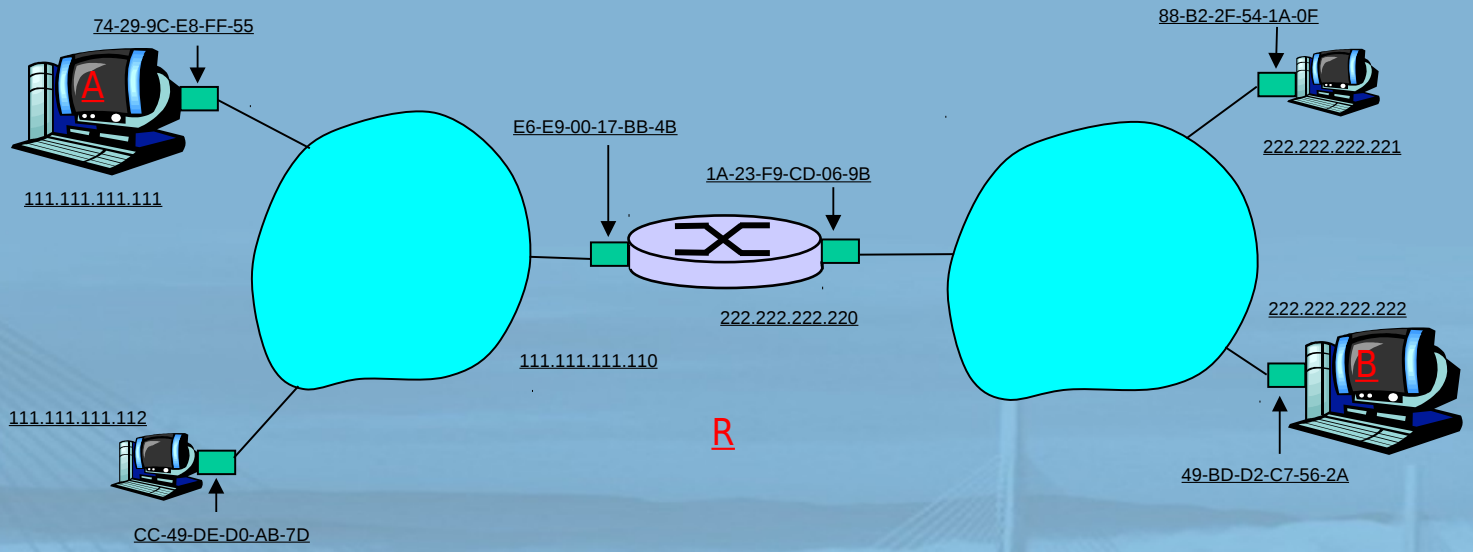
Protocolo ARP: mesma LAN (rede)

- A quer enviar datagrama a B, e endereço MAC de B não está na tabela ARP de A.
- A envia por broadcast pacote de consulta ARP, contendo endereço IP de B
  - endereço MAC de destino = FF-FF-FF-FF-FF-FF
  - todas as máquinas na LAN recebem consulta ARP
- B recebe pacote ARP, responde para A com seu endereço MAC (de B)
  - quadro enviado ao endereço MAC de A (unicast)
- A salva em cache par de endereços IP-para-MAC em sua tabela ARP até a informação expirar
  - estado soft: informação que expira (desaparece) se não for renovada
- ARP é "plug-and-play":
  - nós criam suas tabelas ARP *sem intervenção do administrador de rede*

Endereçamento: roteando para outra LAN

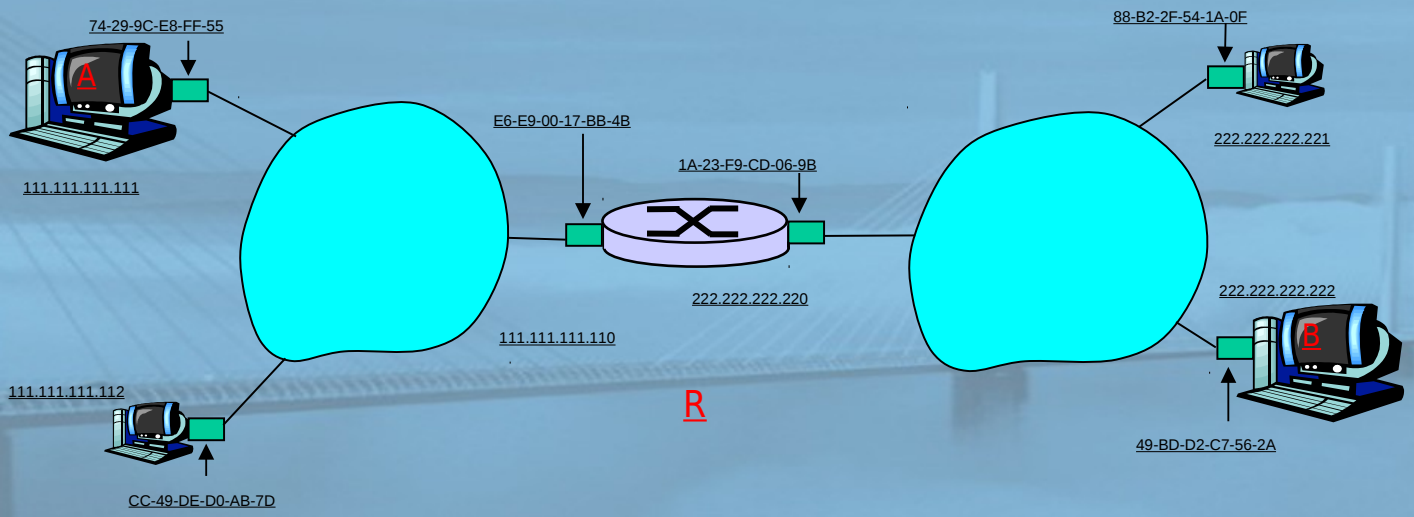
acompanhamento: enviar datagrama de A para B via R

suponha que A saiba o endereço IP de B



- duas tabelas ARP no roteador R, uma para cada rede IP (LAN)

- A cria datagrama IP com origem A, destino B
- A usa ARP para obter endereço MAC de R para 111.111.111.110
- A cria quadro da camada de enlace com endereço MAC de R como destino, quadro contém datagrama IP A-para-B
- NIC de A envia quadro
- NIC de R recebe quadro
- R remove datagrama IP do quadro Ethernet, vê o seu destinado a B
- R usa ARP para obter endereço MAC de B
- R cria quadro contendo datagrama IP A-para-B e envia para B



Endereços IP: como obter um?

P: Como um *hospedeiro* obtém endereço IP?

- fornecido pelo administrador do sistema em um arquivo
  - Linux (Ubuntu): /etc/network/interfaces
- DHCP: Dynamic Host Configuration Protocol: recebe endereço dinamicamente do servidor
  - "plug-and-play"

DHCP: Dynamic Host Configuration Protocol

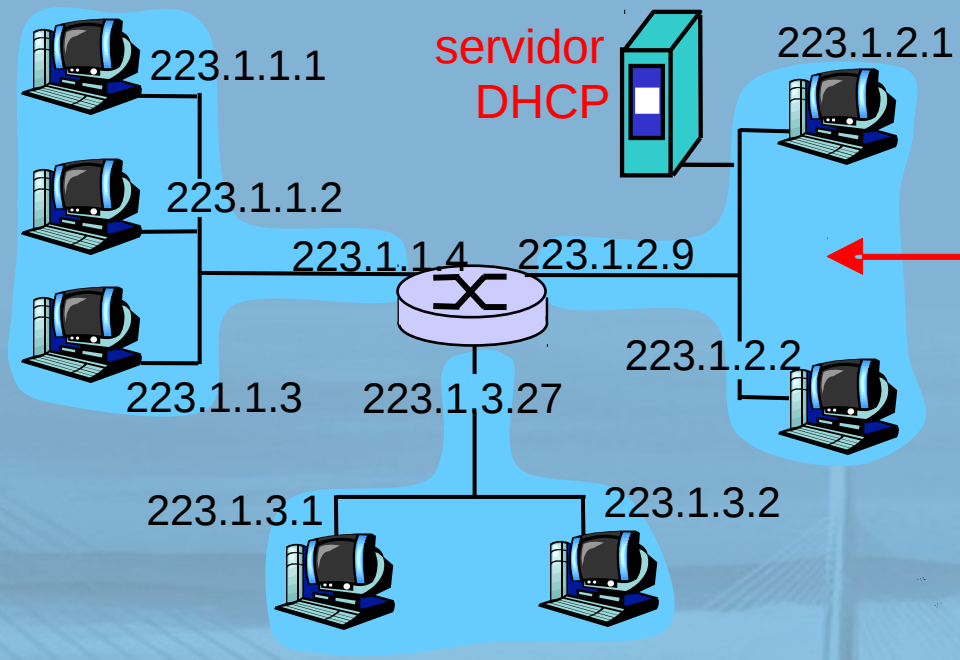
Objetivo: permitir que o hospedeiro obtenha *dinamicamente* seu endereço IP do servidor de rede quando se conectar à rede

- pode renovar seu prazo no endereço utilizado
- permite reutilização de endereços (só mantém endereço enquanto conectado e "ligado")

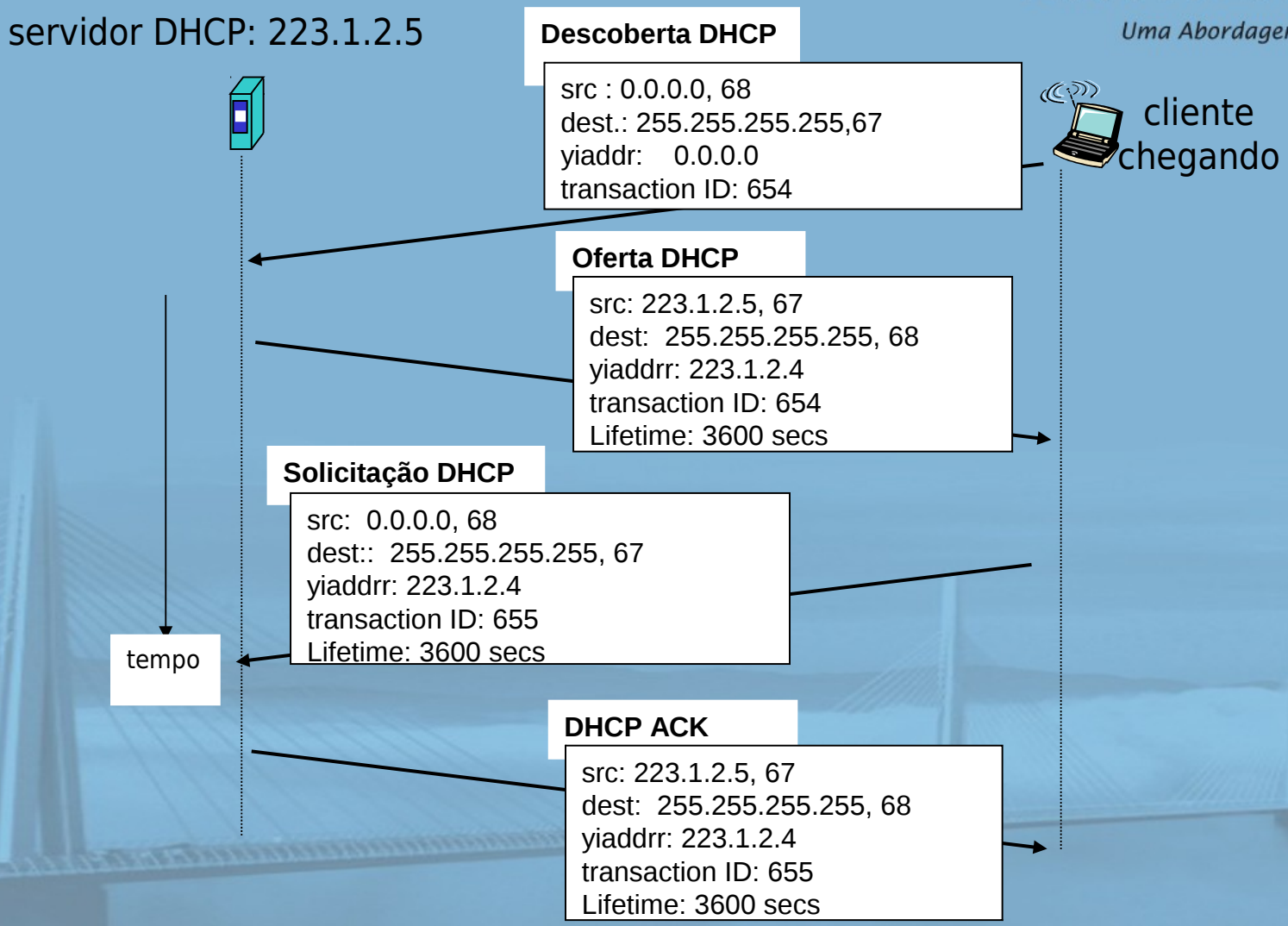
Visão geral do DHCP:

- host broadcasts "DHCP discover" msg [optional]
- servidor DHCP responde com msg "DHCP offer" [opcional]
- hospedeiro requer endereço IP: msg "DHCP request"
- servidor DHCP envia endereço: msg "DHCP ack"

DHCP – cenário cliente/servidor



cliente DHCP chegando precisa de endereço nesta rede

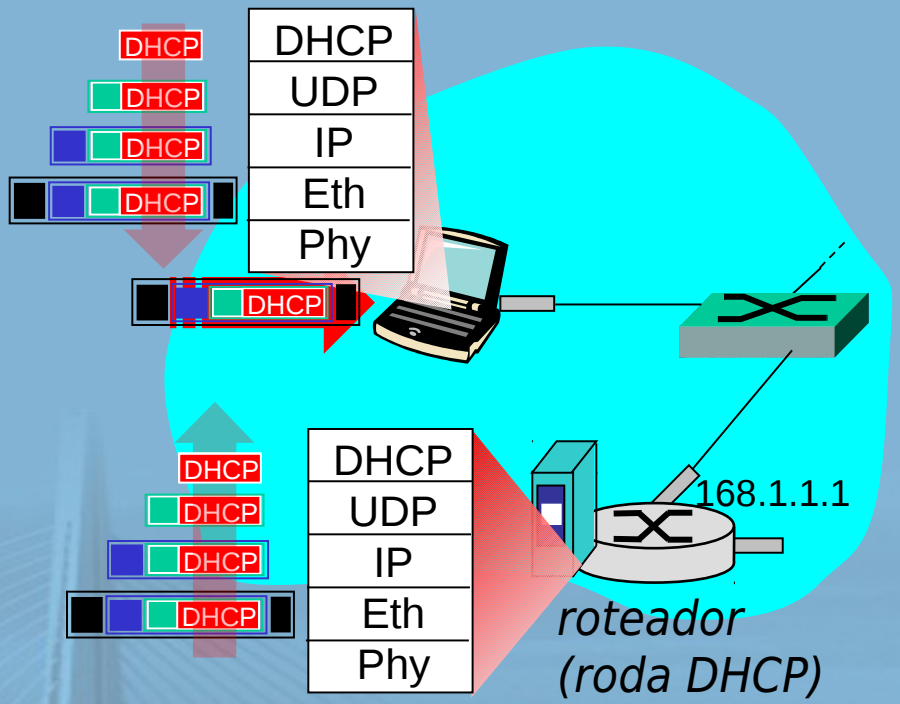


DHCP: mais do que endereço IP

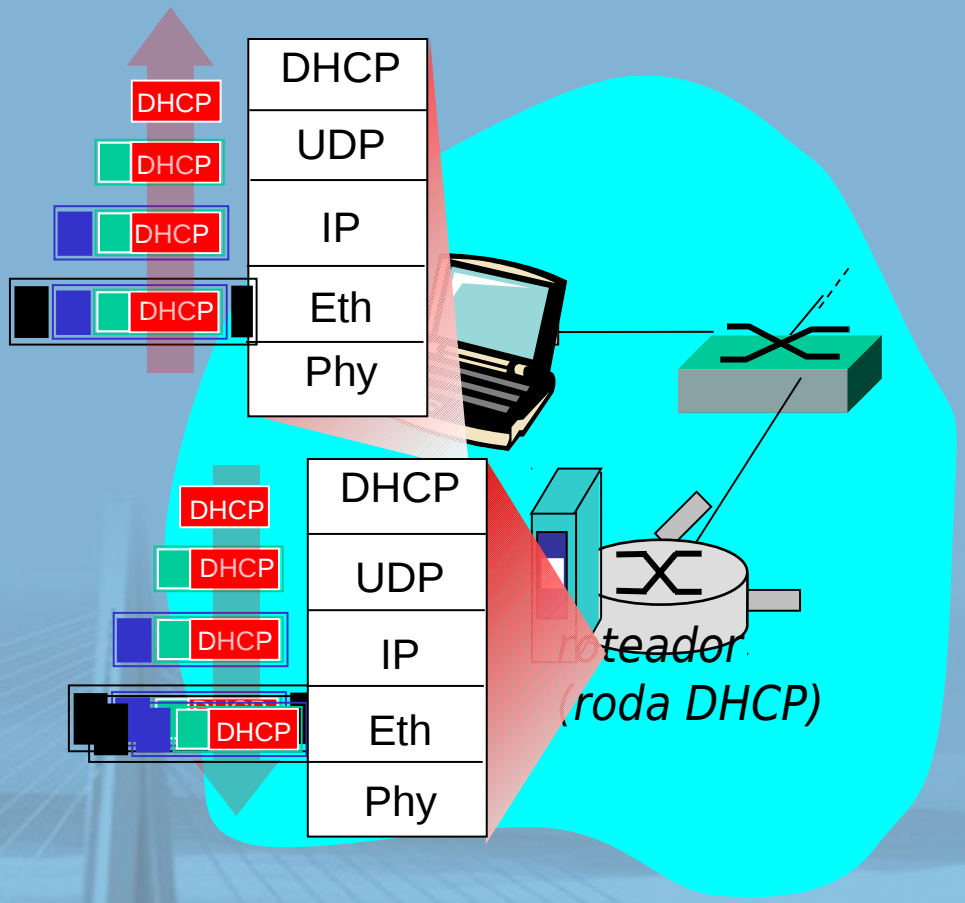
DHCP pode retornar mais do que apenas o endereço IP alocado na sub-rede:

- endereço do roteador do primeiro salto para o cliente
- nome e endereço IP do servidor DNS
- máscara de rede (indicando parte de rede *versus* hospedeiro do endereço)

DHCP: exemplo



- conexão de laptop precisa do seu endereço IP, endereço do roteador do primeiro salto, endereço do servidor DNS: use DHCP
- solicitação DHCP encapsulada no UDP, encapsulada no IP, encapsulado no Ethernet 802.1
- broadcast de quadro Ethernet (dest: FFFFFFFFFFFF) na LAN, recebido no roteador rodando DHCP
- Ethernet demultiplexado para IP demultiplexado, UDP demultiplexado para DHCP



- servidor DCP formula DHCP ACK contendo endereço IP do cliente, endereço IP do roteador do primeiro salto para cliente, nome & endereço IP do servidor DNS
- encapsulamento do servidor DHCP, quadro repassado ao cliente, demultiplexando para DHCP no cliente
- cliente agora sabe seu endereço IP, nome e endereço IP do servidor DSN, endereço IP do seu roteador do primeiro salto

DHCP: Saída wireshark (LAN doméstica)

REDES DE COMPUTADORES E A INTERNET 5ª edição
Uma Abordagem Top-Down

solicitação

Message type: **Boot Request (1)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t = 53,l = 1) **DHCP Message Type = DHCP Request**
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t = 50,l = 4) Requested IP Address = 192.168.1.101
Option: (t = 12,l = 5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    ……

resposta

Message type: **Boot Reply (2)**
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t = 53,l = 1) DHCP Message Type = DHCP ACK
Option: (t = 54,l = 4) Server Identifier = 192.168.1.1
Option: (t = 1,l = 4) Subnet Mask = 255.255.255.0
Option: (t = 3,l = 4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
    IP Address: 68.87.71.226;
    IP Address: 68.87.73.242;
    IP Address: 68.87.64.146
Option: (t = 15,l = 20) Domain Name = "hsd1.ma.comcast.net."

Endereços IP: como obter um?

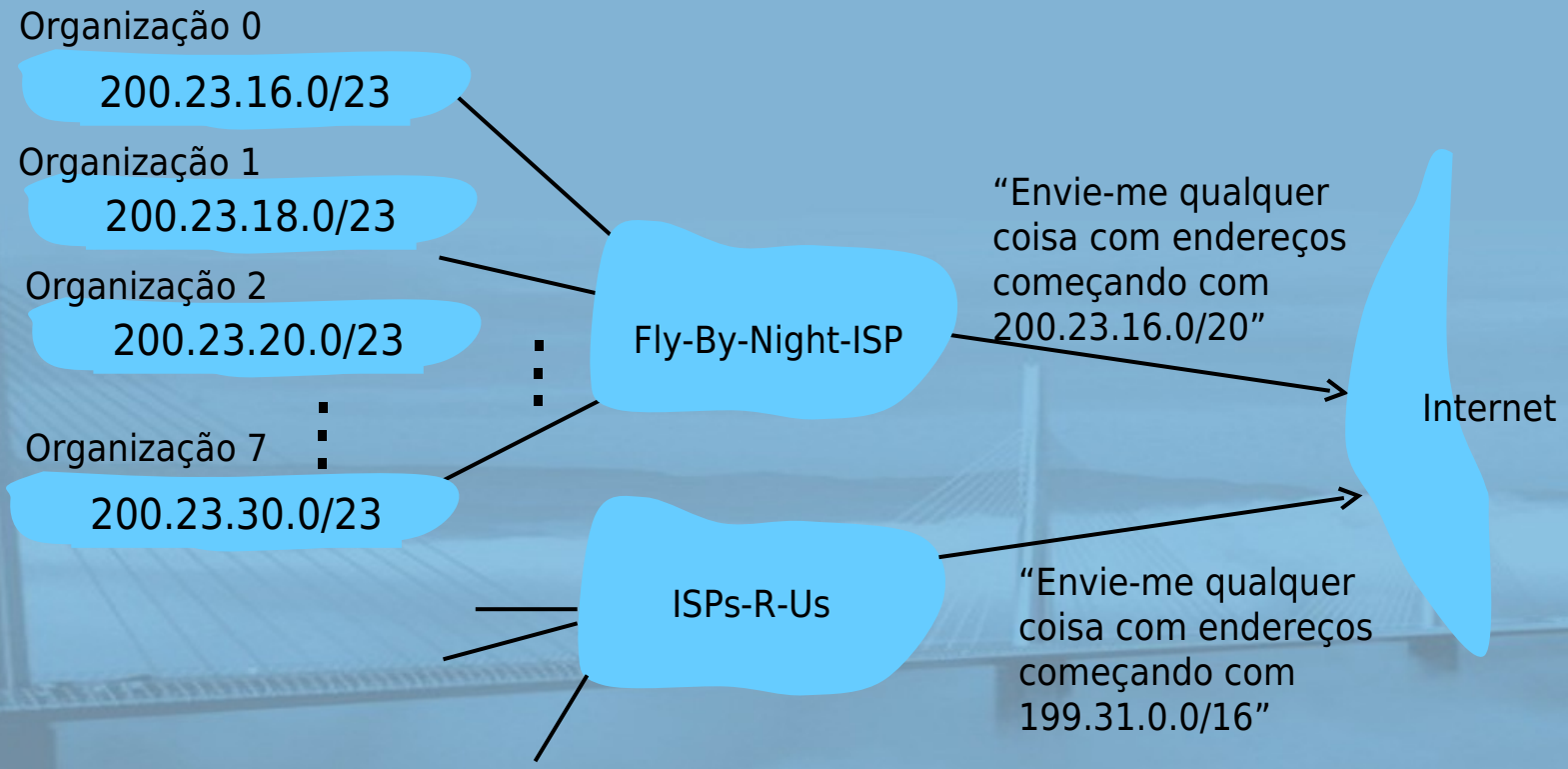
P: Como a *rede* obtém a parte de sub-rede do endereço IP?

R: Recebe parte alocada do espaço de endereços do seu ISP

Bloco do ISP	11001000 00010111 00010000	00000000	200.23.16.0/20
Organização 0	11001000 00010111 0001000**0**	00000000	200.23.16.0/23
Organização 1	11001000 00010111 0001001**0**	00000000	200.23.18.0/23
Organização 2	11001000 00010111 0001010**0**	00000000	200.23.20.0/23
...	.....	....	....
Organização 7	11001000 00010111 0001111**0**	00000000	200.23.30.0/23

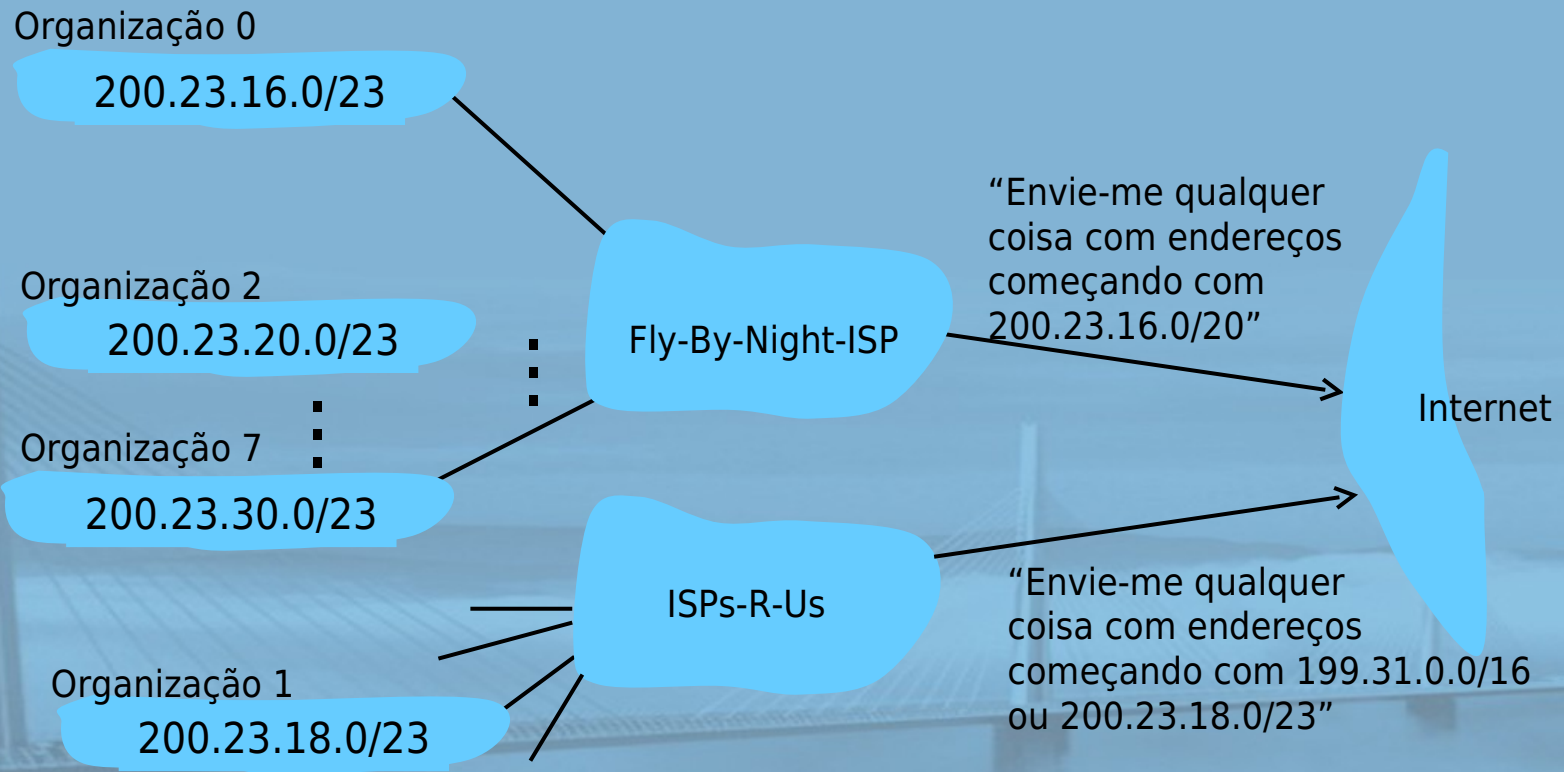
Endereçamento hierárquico: agregação de rota

Endereçamento hierárquico permite anúncio eficiente da informação de roteamento:



Endereçamento hierárquico: rotas mais específicas

ISPs-R-Us tem uma rota mais específica para Organização 1



Endereçamento IP: a última palavra...

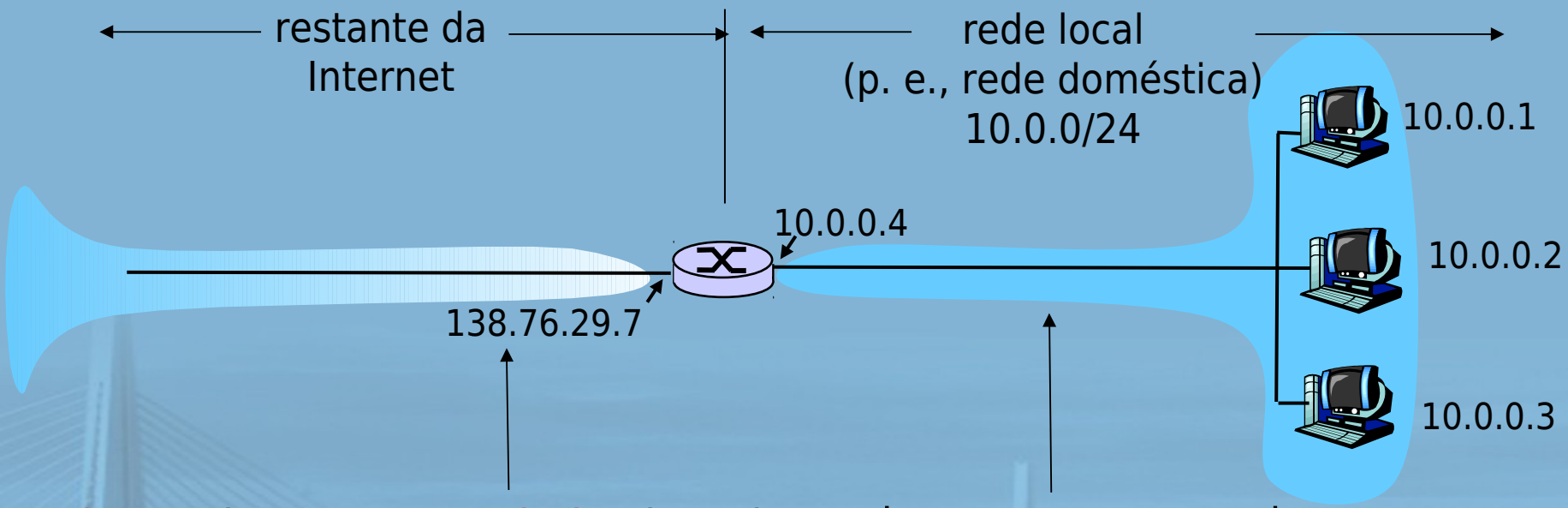
P: Como um ISP recebe bloco de endereços?

R: ICANN: Internet Corporation for Assigned Names and Numbers

- aloca endereços
- administra o DNS
- atribui nomes de domínio e resolve disputas

NAT: Network Address Translation

REDES DE COMPUTADORES E A INTERNET 5ª edição
Uma Abordagem Top-Down



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)

- 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

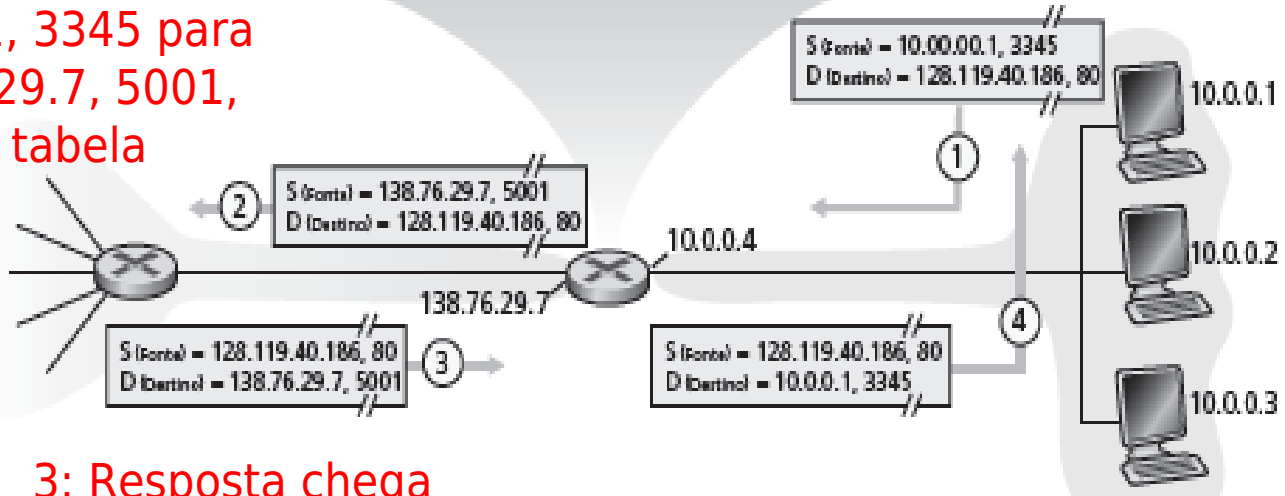
- *lembrar (na tabela de tradução NAT)* de cada par de tradução (endereço IP de origem, # porta) para (endereço IP da NAT, novo # porta)

- *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

Tabela de tradução NAT	
Lado da WAN	Lado da LAN
138.76.29.7, 5001	10.0.0.1, 3345
...	...

1: hospedeiro 10.0.0.1 envia datagrama para 128.119.40.186, 80



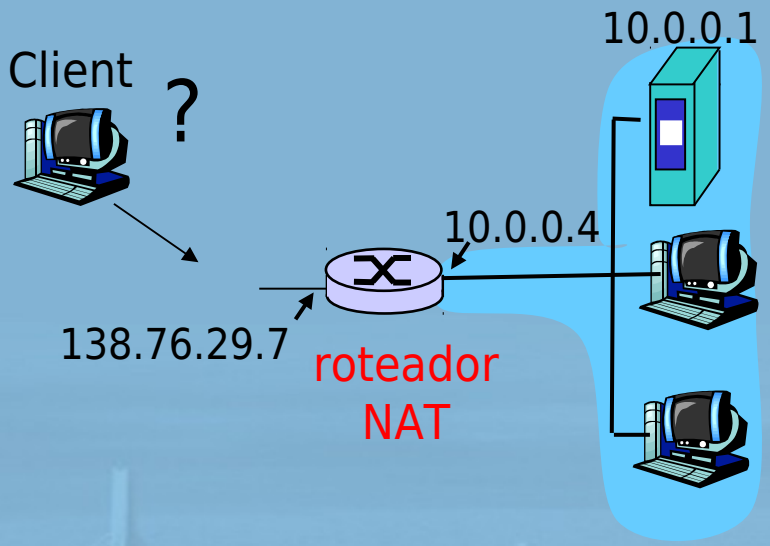
3: Resposta chega endereço destino: 138.76.29.7, 5001

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 controvertido:
  - 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

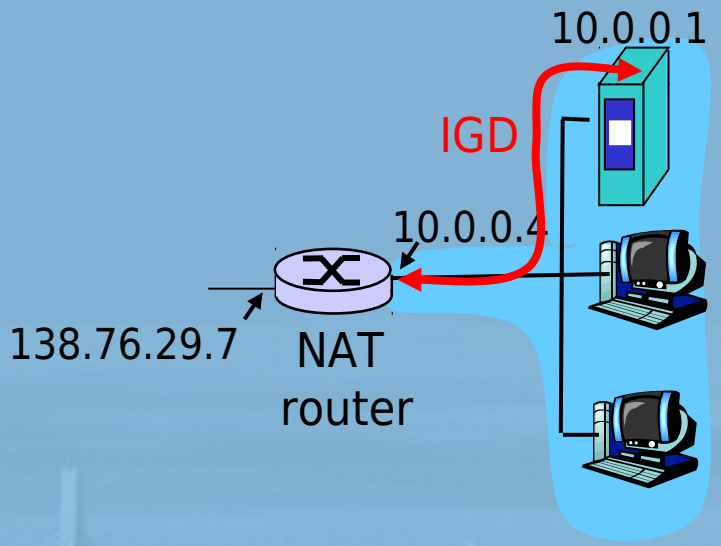
Problema da travessia da NAT

- 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

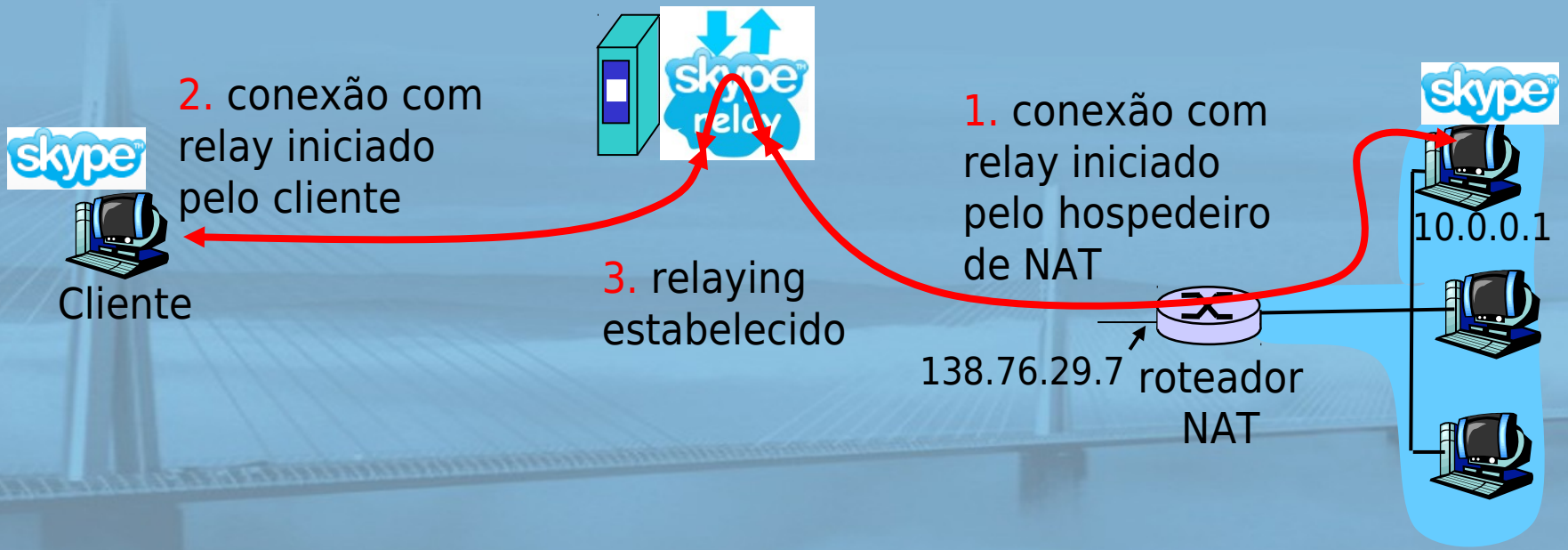


- solução 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Permite que o hospedeiro com NAT:
  - descubra endereço IP público (138.76.29.7)
  - inclua/remova mapeamentos de porta (com tempos de posse)

ou seja, automatizar configuração estática do mapa de porta NAT

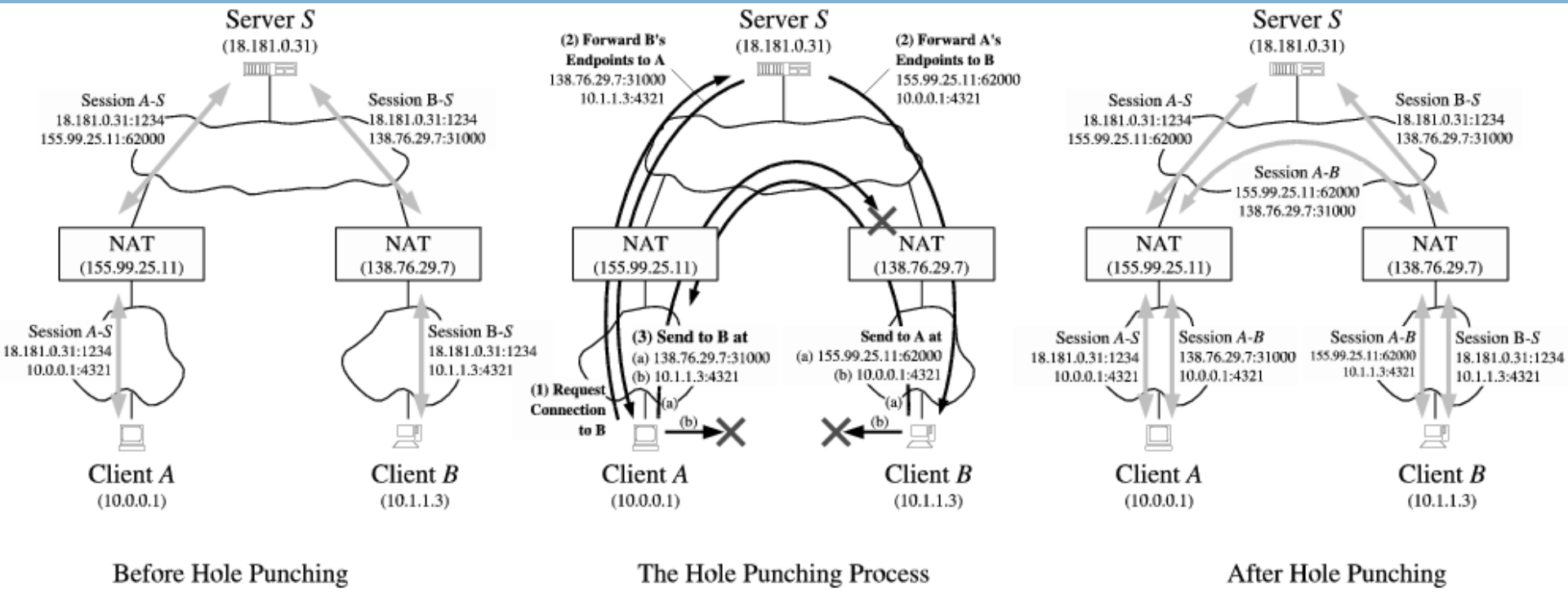


- solução 3: repasse (usado no Skype)
  - cliente com NAT estabelece conexão com repasse
  - cliente externo se conecta ao repasse
  - repasse liga pacotes entre duas conexões

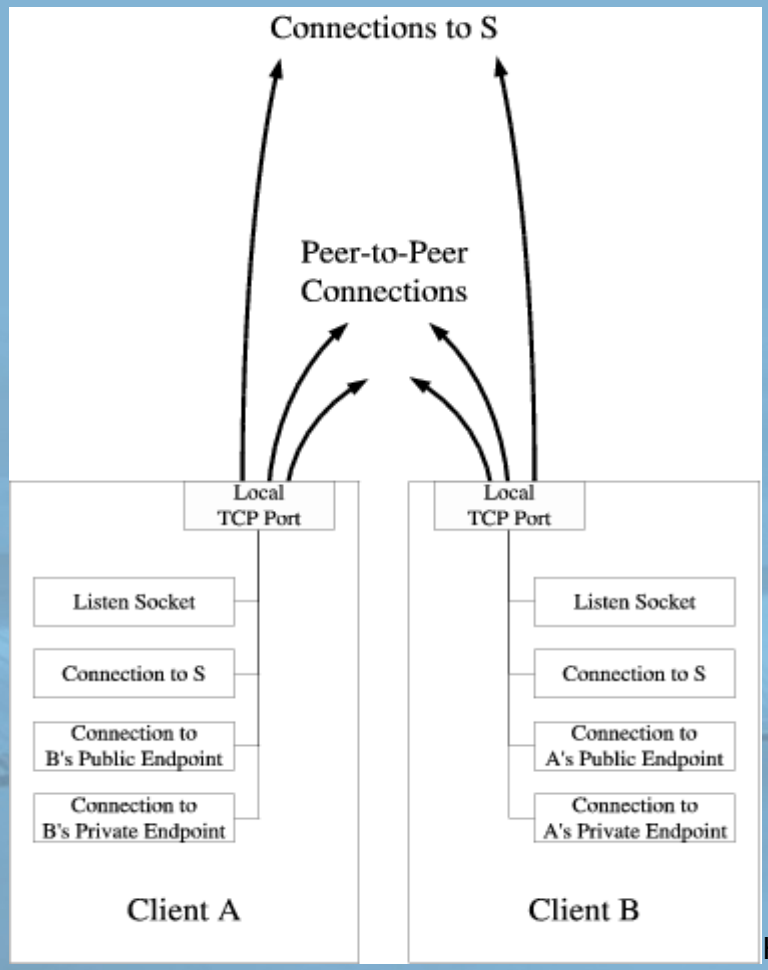


- solução 4: Hole Punching
  - Tipos de NAT
    - full cone: mapeamento um para um (**OK**)
      - iAddr:iPort ↔ eAddr:ePort
      - qualquer hospedeiro destino
    - (addres- ou port-) restricted cone (**OK**)
      - iAddr:iPort ↔ eAddr:ePort
      - hospedeiro destino para quem foi enviado pacotes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

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



- Hole Punching em TCP
  - Implementação TCP feita no SO
  - connect() → listen() e accept()
  - reutilização de endereço e porta para conexões



Capítulo 4: Camada de rede

REDES DE COMPUTADORES E A INTERNET 5ª edição
Uma Abordagem Top-Down

- 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

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

REDES DE COMPUTADORES E A INTERNET 5ª edição
Uma Abordagem Top-Down

- 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

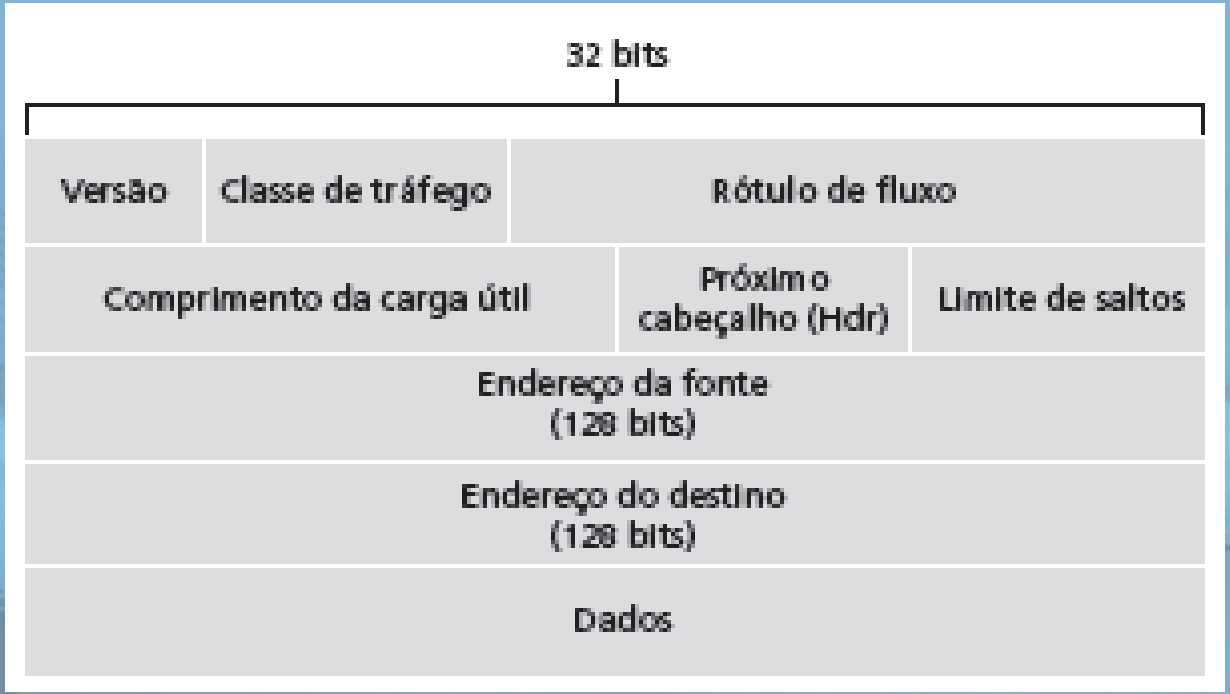
- motivação inicial: espaço de endereço de 32 bit logo estará completamente alocado
- motivação adicional:
  - formato de cabeçalho ajuda a agilizar processamento e repasse
  - mudanças para facilitar QoS

formato de datagrama IPv6:

  - cabeçalho de 40 bytes de tamanho fixo
  - fragmentação não permitida

Cabeçalho IPv6

prioridade: identificar prioridade entre datagramas no fluxo
rótulo de fluxo: identificar datagramas no mesmo "fluxo." (conceito de "fluxo" não bem definido)
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

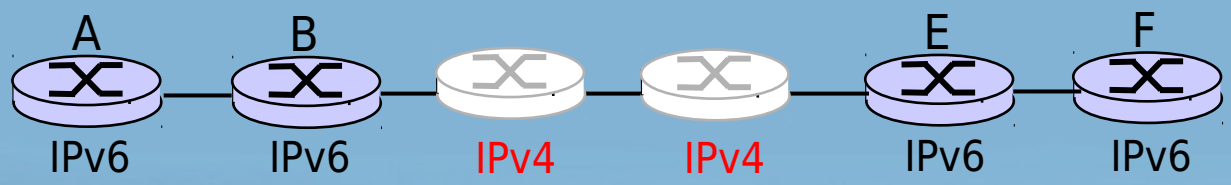
Transição de IPv4 para IPv6

- 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

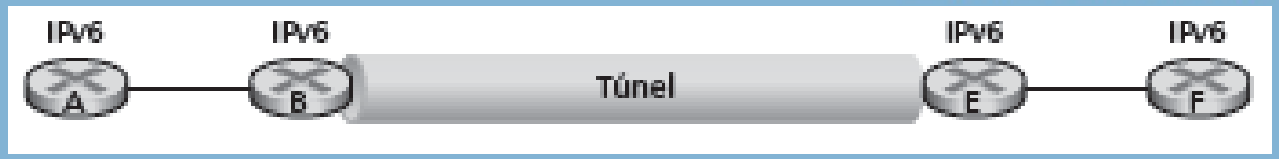
Implantação de túnel

Visão lógica:

Visão física:



Visão lógica:



Visão física: