

Endereços IP: como obter um?

- Na verdade, são **duas** perguntas:
 1. Como um host obtém o endereço IP dentro de sua rede (parte do host do endereço)?
 2. Como uma rede obtém o endereço IP para si mesma (parte da rede do endereço)
- Como o host obtém o endereço IP?
 - Codificado pelo sysadmin no arquivo de config (e.g., /etc/rc.config no UNIX)
 - **DHCP: Dynamic Host Configuration Protocol**: obtém o endereço dinamicamente do servidor
 - “plug-and-play”

DHCP: Dynamic Host Configuration Protocol

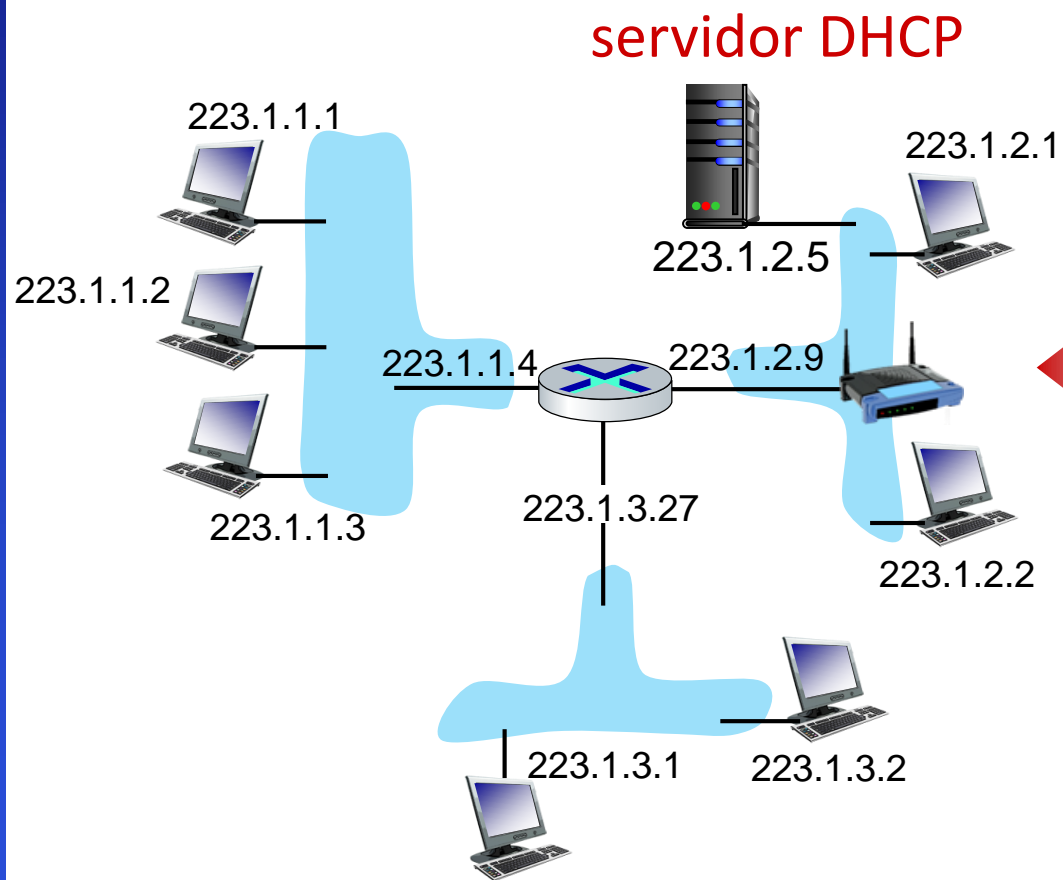
Objetivo: host obtém dinamicamente o endereço IP do servidor de rede quando ele “ingressa” na rede

- pode renovar sua “locação” no endereço em uso
- permite a reutilização de endereços (mantém o endereço apenas enquanto estiver conectado/ligado)
- suporte para vários usuários móveis que ingressam/saem da rede

- Visão geral do DHCP:

- hosts fazem broadcast de mensagem de **descoberta DHCP** (opcional)
- servidor DHCP responde com a mensagem de **oferta DHCP** (opcional)
- host solicita endereço IP: mensagem de **requisição DHCP**
- servidor DHCP envia o endereço: mensagem **ack DHCP**

Cenário cliente-servidor DHCP



Normalmente, o servidor DHCP está co-localizado no roteador, servindo todas as sub-redes às quais o roteador está conectado



cliente DHCP necessita de endereço nesta rede

Cenário cliente-servidor DHCP

servidor DHCP: 223.1.2.5

Descoberta DHCP

Broadcast: existe um servidor DHCP por aí?

cliente

Oferta DHCP

Broadcast: Eu sou um servidor DHCP! Segue um endereço IP que você pode usar

Requisição DHCP

Broadcast: OK. Gostaria de usar este endereço IP!

ACK DHCP

Broadcast: OK. Você tem esse endereço IP!

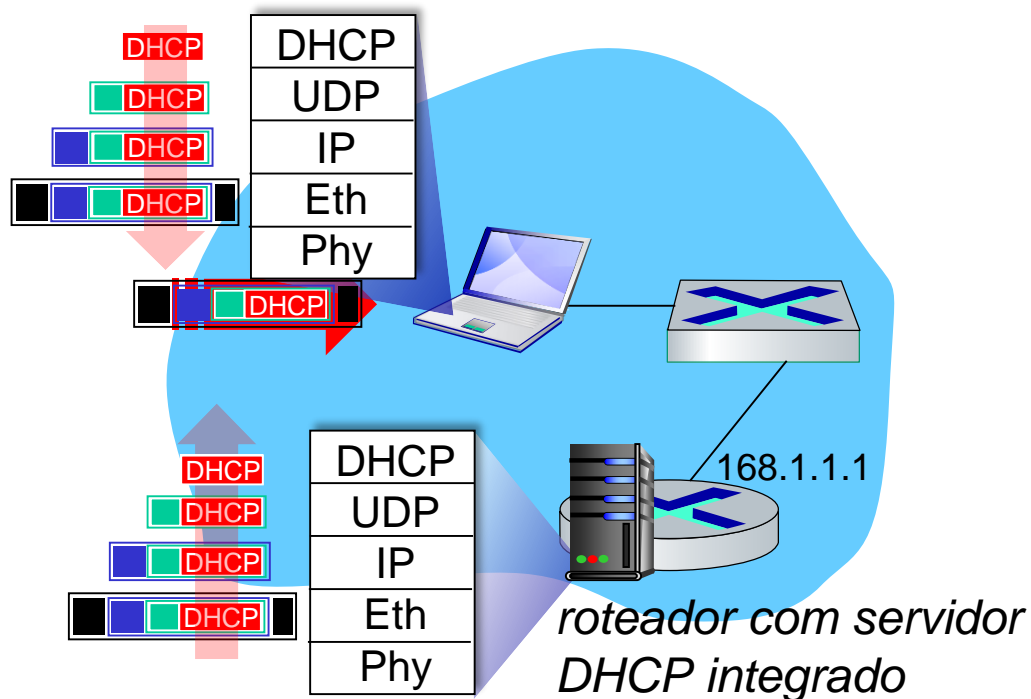
As duas etapas acima podem ser ignoradas "se um cliente se lembrar e desejar reutilizar um endereço de rede alocado anteriormente" [RFC 2131]

DHCP: mais do que endereços IP

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

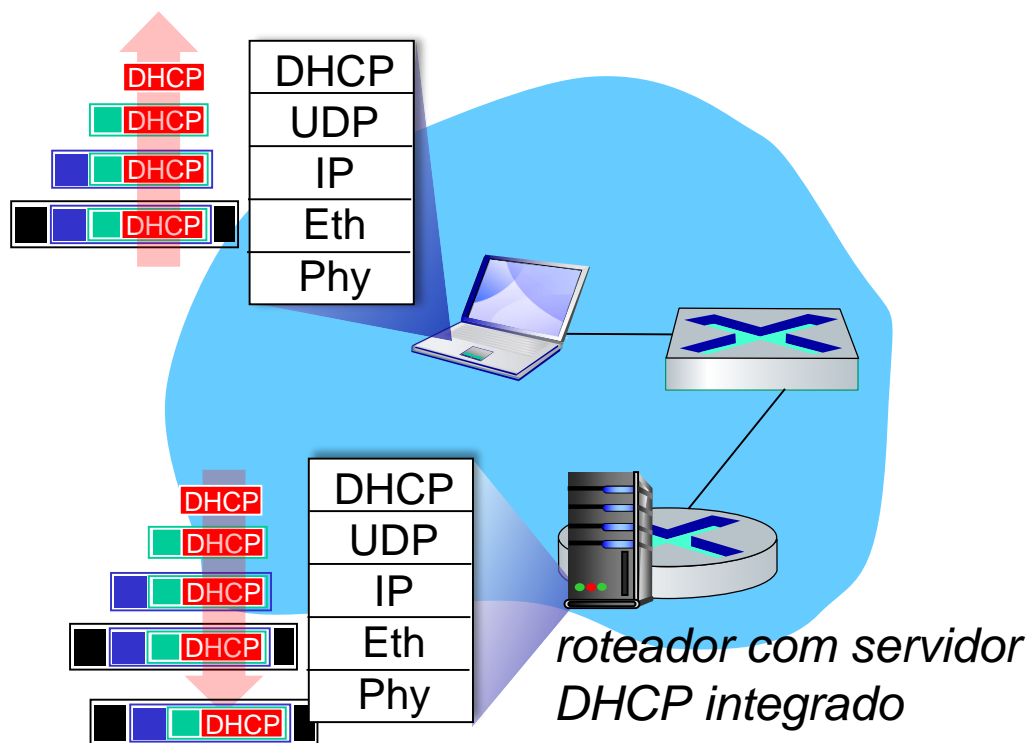
- endereço do roteador de primeiro salto para o cliente
- nome e endereço IP do servidor DNS
- máscara de rede (indicando partes, redes x host, do endereço)

DHCP: exemplo



- Laptop usará DHCP para obter endereço IP, endereço do roteador de primeiro salto, endereço do servidor DNS.
- Mensagem DHCP REQUEST encapsulada em UDP, encapsulada em IP, encapsulada em Ethernet
- Transmissão de quadro Ethernet (dest: FFFFFFFFFFFFFFFF) na LAN, recebida no roteador que executa o servidor DHCP
- Ethernet de-muxe para IP de-muxe, UDP de-muxe para DHCP

DHCP: exemplo



- O servidor DHCP cria o ACK DHCP contendo o endereço IP do cliente, o endereço IP do roteador de primeiro salto para o cliente, o nome e o endereço IP do servidor DNS
- resposta encapsulada do servidor DHCP encaminhada para o cliente, de-muxing até DHCP no cliente
- o cliente agora sabe seu endereço IP, nome e endereço IP do servidor DNS, endereço IP de seu roteador de primeiro salto

Endereços IP: como obter um?

Pergunta: como a rede obtém a parte da sub-rede do endereço IP?

Resposta: obtém a parte alocada do espaço de endereços do ISP

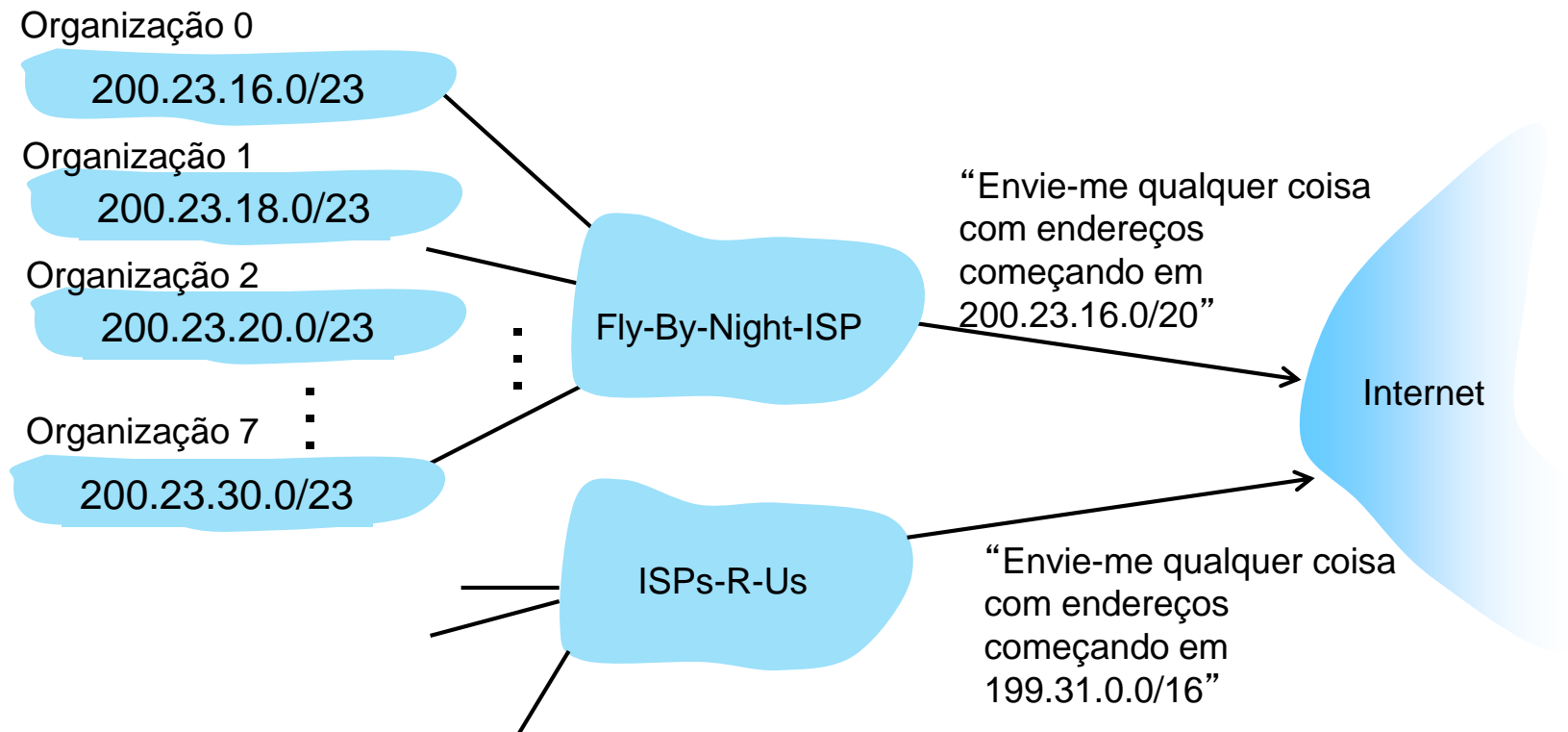
Bloco do ISP 11001000 00010111 00010000 00000000 200.23.16.0/20

O ISP pode então alocar seu espaço de endereço em 8 blocos:

Organização 0	<u>11001000 00010111 00010000</u>	00000000	200.23.16.0/23
Organização 1	<u>11001000 00010111 00010010</u>	00000000	200.23.18.0/23
Organização 2	<u>11001000 00010111 00010100</u>	00000000	200.23.20.0/23
...			
Organização 7	<u>11001000 00010111 00011110</u>	00000000	200.23.30.0/23

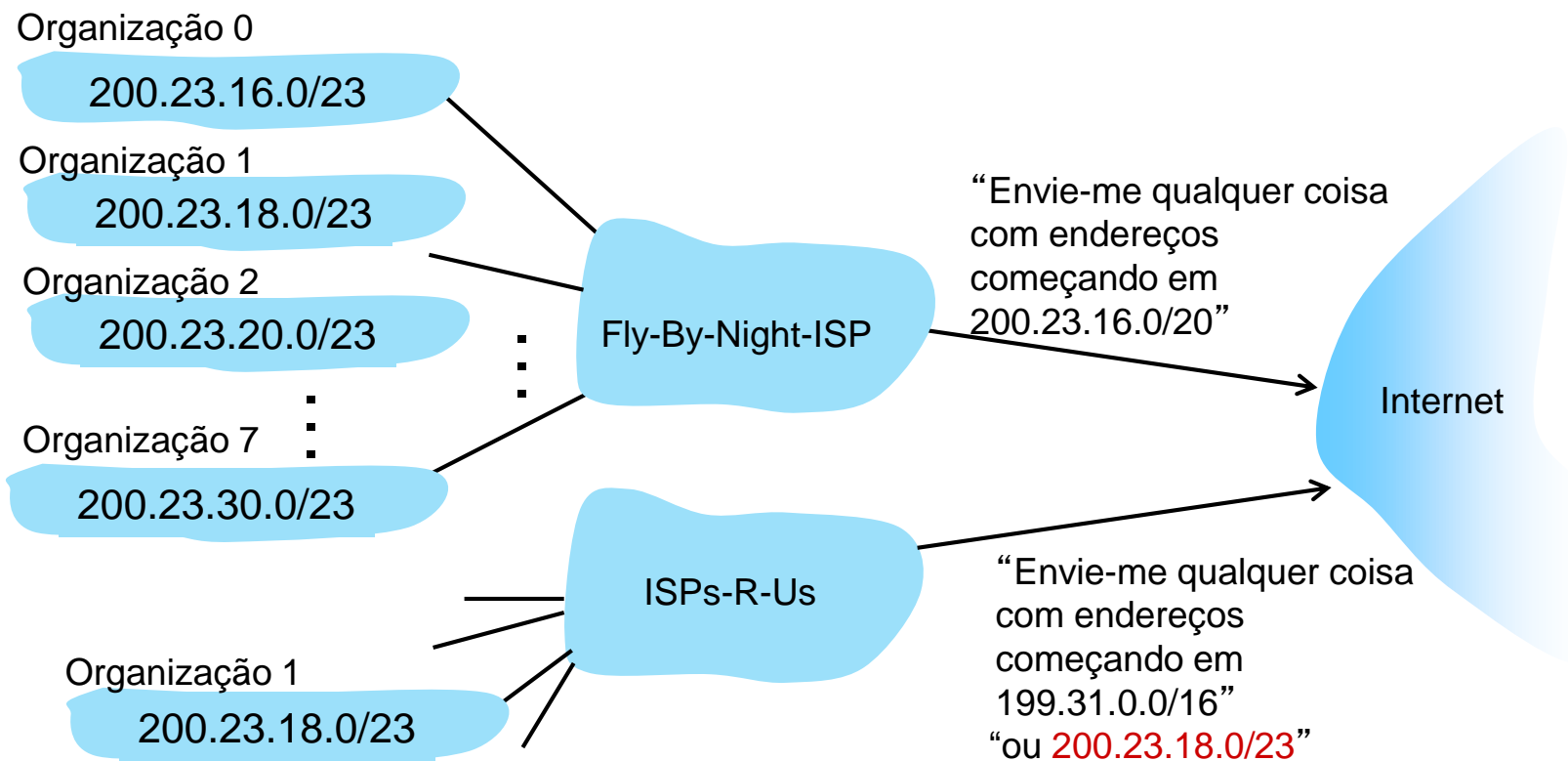
Endereços hierárquico: agregação de rotas

O endereçamento hierárquico permite anúncio eficiente das informações de roteamento:



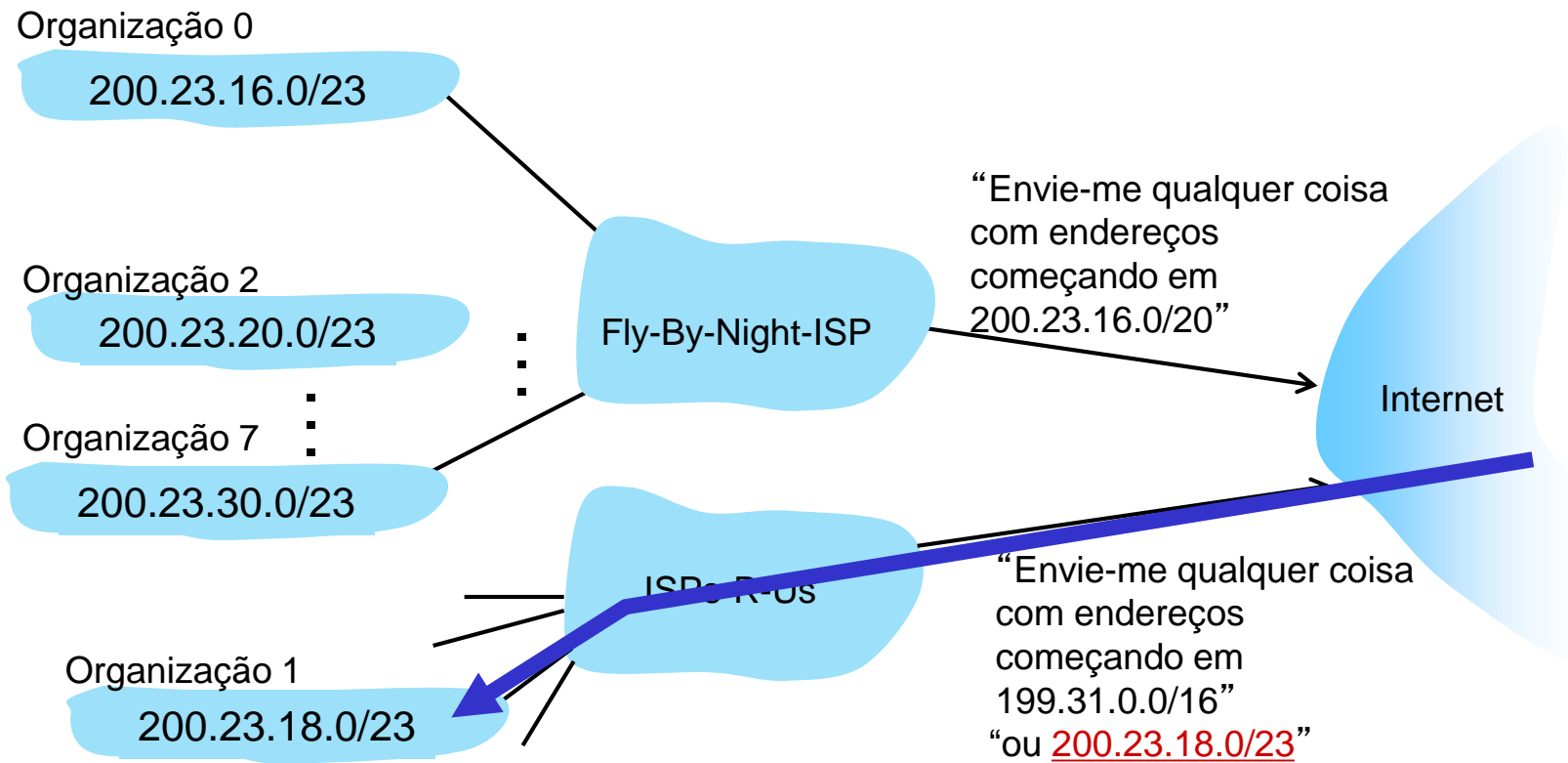
Endereços hierárquico: rotas mais específicas

- A organização 1 muda de Fly-By-Night-ISP para ISPs-R-Us
- ISPs-R-Us agora anuncia rota mais específica para a Organização 1



Endereços hierárquico: rotas mais específicas

- A organização 1 muda de Fly-By-Night-ISP para ISPs-R-Us
- ISPs-R-Us agora anuncia rota mais específica para a Organização 1



Endereçamento IP: considerações finais

Pergunta: como um ISP obtém um bloco de endereços?

Resposta: ICANN: Internet Corporation for Assigned Names and Numbers

<http://www.icann.org>

- aloca endereços IP por 5 ***regional registries (RRs)*** (os quais podem fazer alocações para registros locais)
- gerencia zona raiz do DNS, incluindo delegação do gerenciamento de TLDs individuais (.com, .edu, ...)

Endereçamento IP: considerações finais

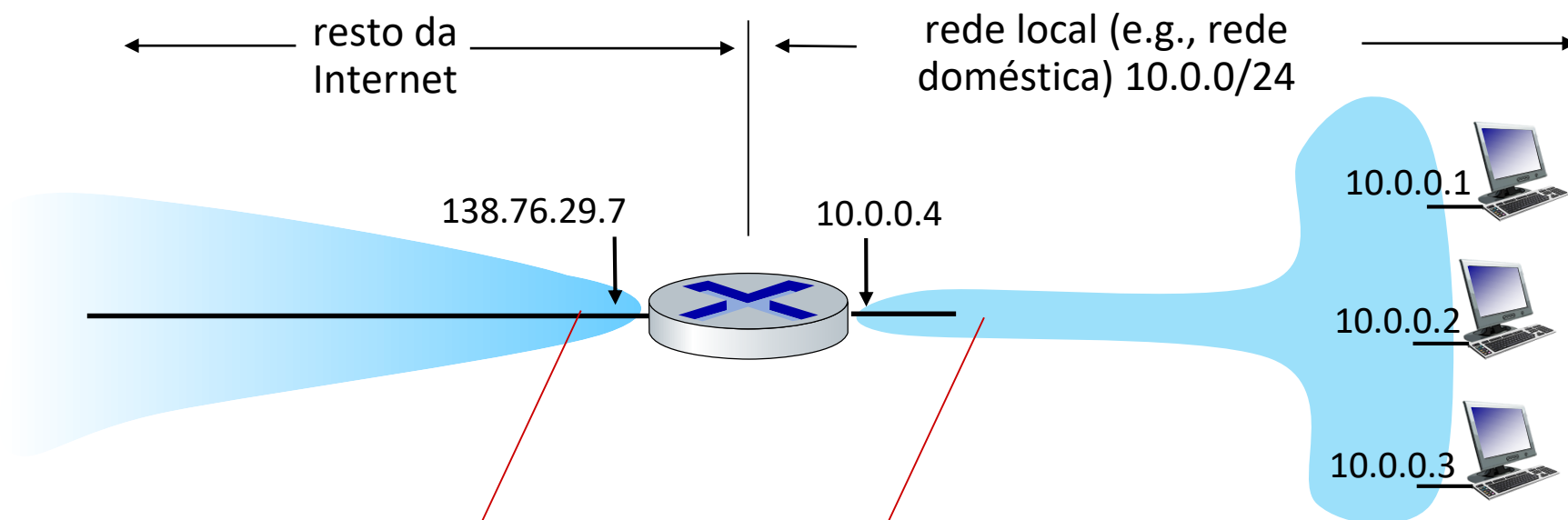
Pergunta: existem endereços IP de 32 bits suficientes?

- ICANN alocou o último bloco de endereços IPv4 para RRs em 2011
- NAT (estudado na próxima aula) ajuda com o problema de exaustão do espaço de endereços IPv4
- IPv6 possui espaço de endereços de 128 bits

“Quem diabos sabia o quanto de espaço de endereços precisávamos?” Vint Cerf (refletindo sobre a decisão de tornar o tamanho do endereço IPv4 32 bits)

NAT: conversão de endereços de rede

NAT (Network Address Translation): todos os dispositivos na rede local compartilham apenas **um** endereço IPv4 no que diz respeito ao mundo externo



todos os datagramas que saem da rede local têm o mesmo endereço IP NAT origem: 138.76.29.7, mas nº de porta origem diferentes

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

NAT: conversão de endereços de rede

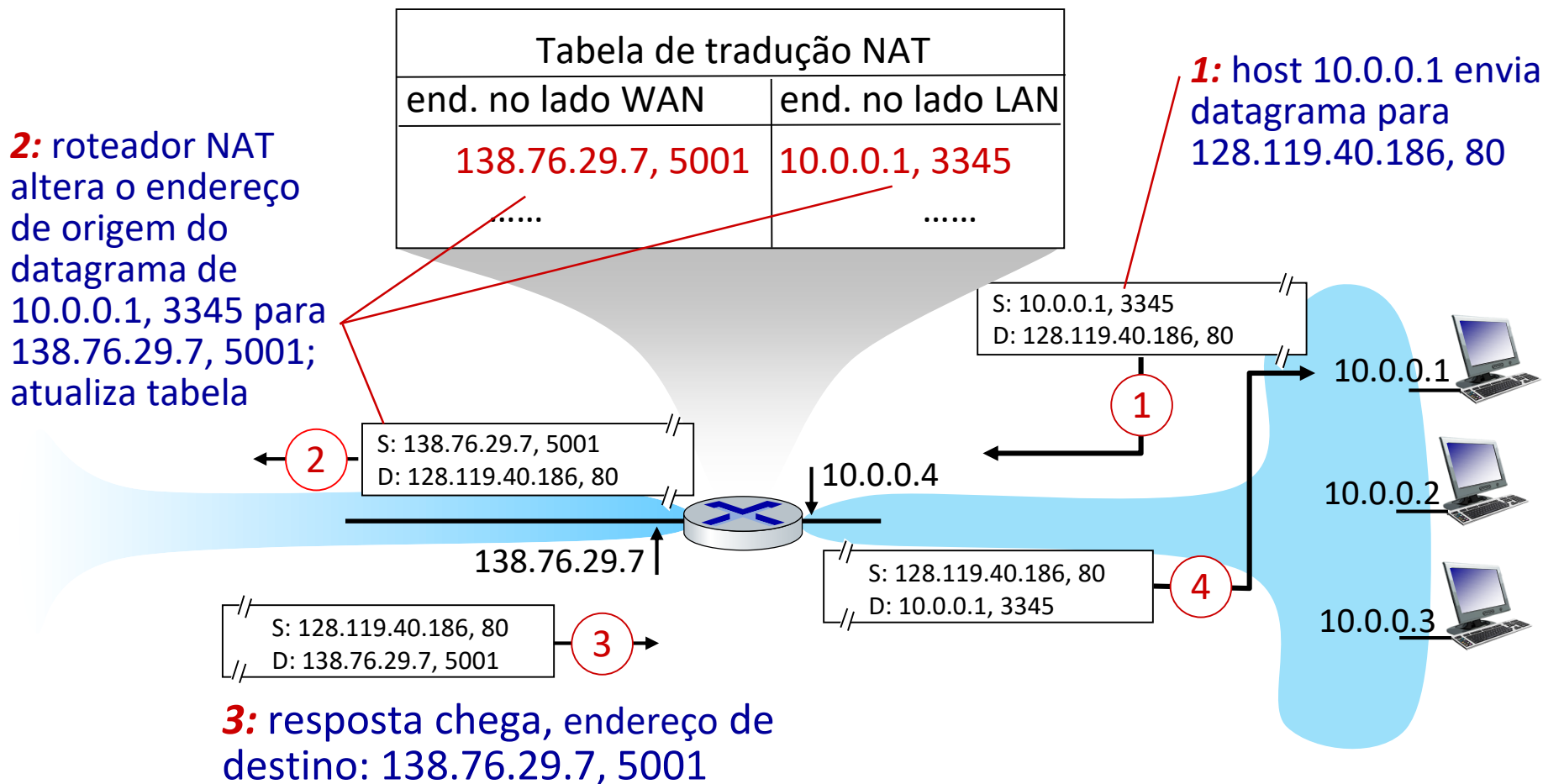
- Todos os dispositivos na rede local têm endereços de 32 bits em um espaço de endereço IP “privado” (prefixos 10/8, 172.16/12, 192.168/16) que só podem ser usados na rede local
- Vantagens:
 - Necessário apenas **um** endereço IP do ISP para todos os dispositivos
 - Pode alterar endereço de host na rede sem notificar o mundo externo
 - Pode alterar o ISP sem alterar endereços de dispositivos de rede local
 - Segurança: dispositivos dentro da rede local não são endereçáveis/visíveis diretamente, pelo mundo exterior

NAT: conversão de endereços de rede

Implementação: o roteador NAT deve (de forma transparente):

- **Datagramas de saída: substituir** (endereço IP de origem, número de porta) de cada datagrama de saída para (endereço IP NAT, novo número de porta)
 - Clientes/servidores remotos responderão usando (endereço IP NAT, novo número de porta) como endereço de destino
- **Lembrar (na tabela de tradução NAT)** cada par (endereço IP de origem, número de porta) para (endereço IP NAT, novo número de porta)
- **Datagramas de entrada: substituir** (endereço IP NAT, novo número de porta) nos campos de destino de cada datagrama de entrada com correspondente (endereço IP de origem, número de porta) armazenado na tabela NAT

NAT: conversão de endereços de rede



NAT: conversão de endereços de rede

- NAT é controverso:
 - roteadores “devem” processar apenas até a camada 3
 - “escassez” de endereços deve ser resolvida pelo IPv6
 - viola o argumento de ponta a ponta (manipulação do número de porta pelo dispositivo da camada de rede)
 - NAT Transversal (NAT-T): e se um cliente externo quiser se conectar ao servidor atrás de um NAT? (e.g. P2P, videoconferência, jogos eletrônicos)
- Mas o NAT veio para ficar:
 - amplamente utilizado em redes domésticas e institucionais, redes celulares 4G/5G

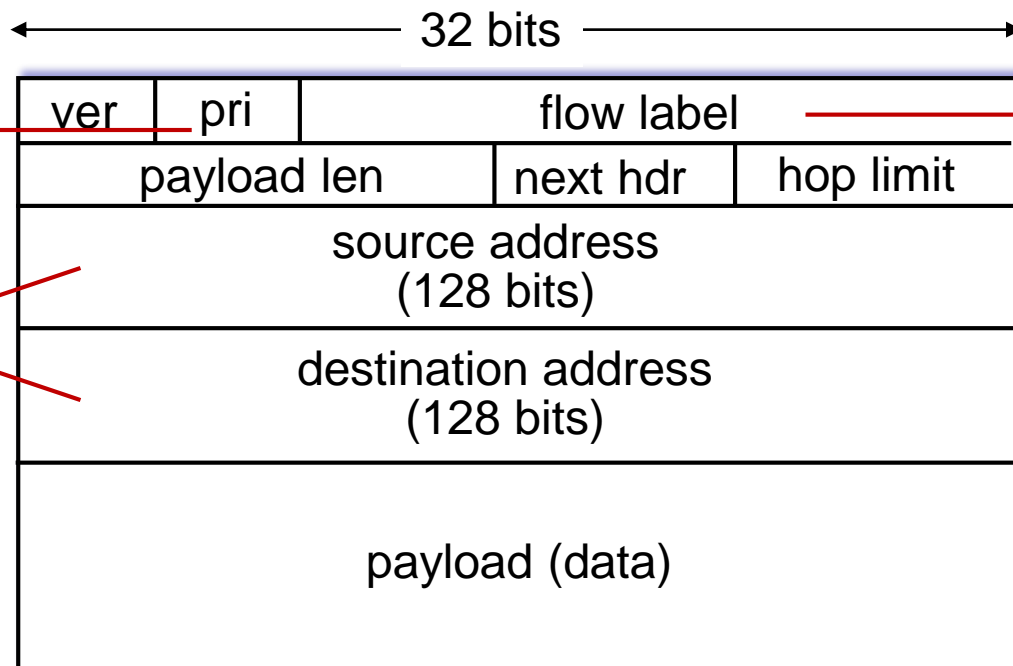
IPv6: motivação

- **Motivação inicial:** o espaço de endereços IPv4 de 32 bits seria esgotado
- Motivação adicional:
 - velocidade de processamento/encaminhamento: cabeçalhos de comprimento fixo de 40 bytes
 - permitir o tratamento de diferentes camadas de rede de “fluxos”

Formato de datagrama IPv6

prioridade: identificar
prioridade entre
datagramas no fluxo

endereços IPv6
de 128-bit



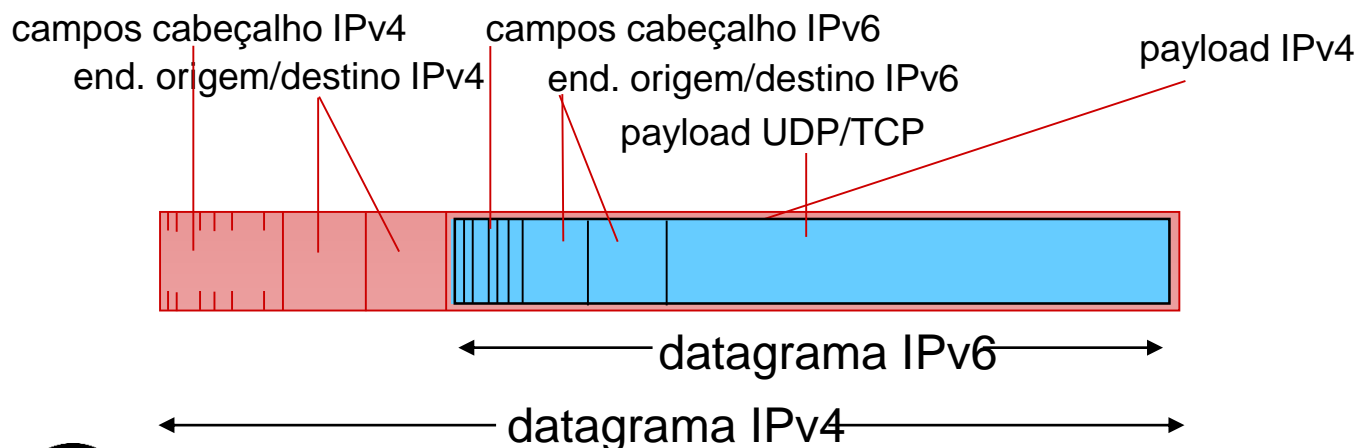
etiqueta de fluxo:
identifique datagramas no mesmo "fluxo".
(conceito de "fluxo" não bem definido).

O que está faltando (em comparação com o IPv4):

- sem soma de verificação (para acelerar o processamento em roteadores)
- sem fragmentação/remontagem
- sem opções (disponível como protocolo de camada superior)

Transição do IPv4 para o IPv6

- Nem todos os roteadores podem ser atualizados simultaneamente
 - Como a rede funcionará com roteadores IPv4 e IPv6 mistos?
- Tunelamento: datagrama IPv6 transportado como carga útil no datagrama IPv4 entre roteadores IPv4 (“pacote dentro de um pacote”)
 - Tunelamento usado extensivamente em outros contextos (4G/5G)



Tunelamento e encapsulamento

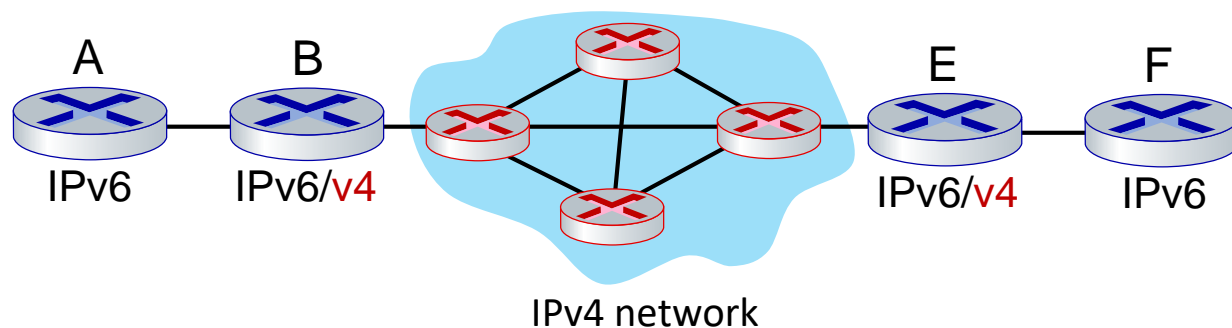
Ethernet
conectando dois
roteadores IPv6:



quadro da camada de enlace

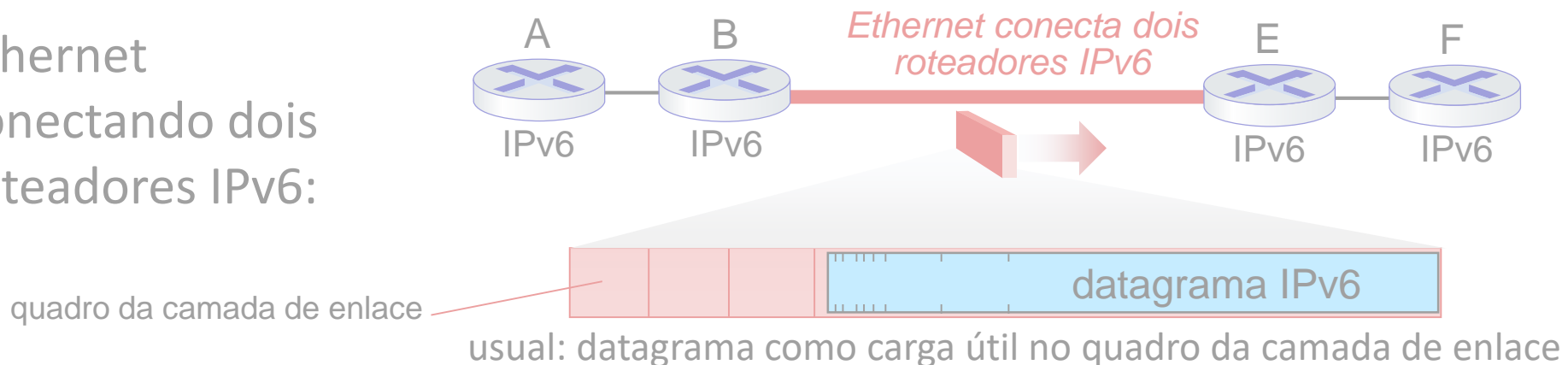
usual: datagrama como carga útil no quadro da camada de enlace

Rede IPv4
conectando dois
roteadores IPv6

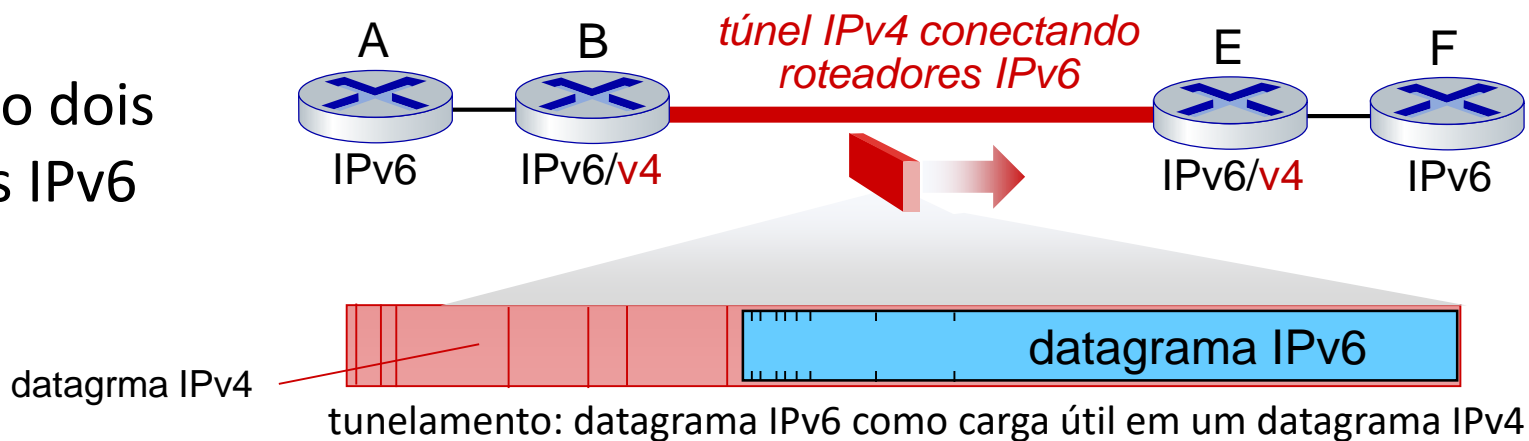


Tunelamento e encapsulamento

Ethernet
conectando dois
roteadores IPv6:



Túnel IPv4
conectando dois
roteadores IPv6

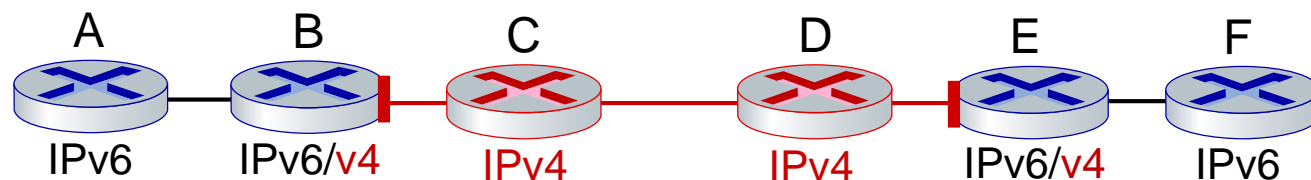


Tunelamento

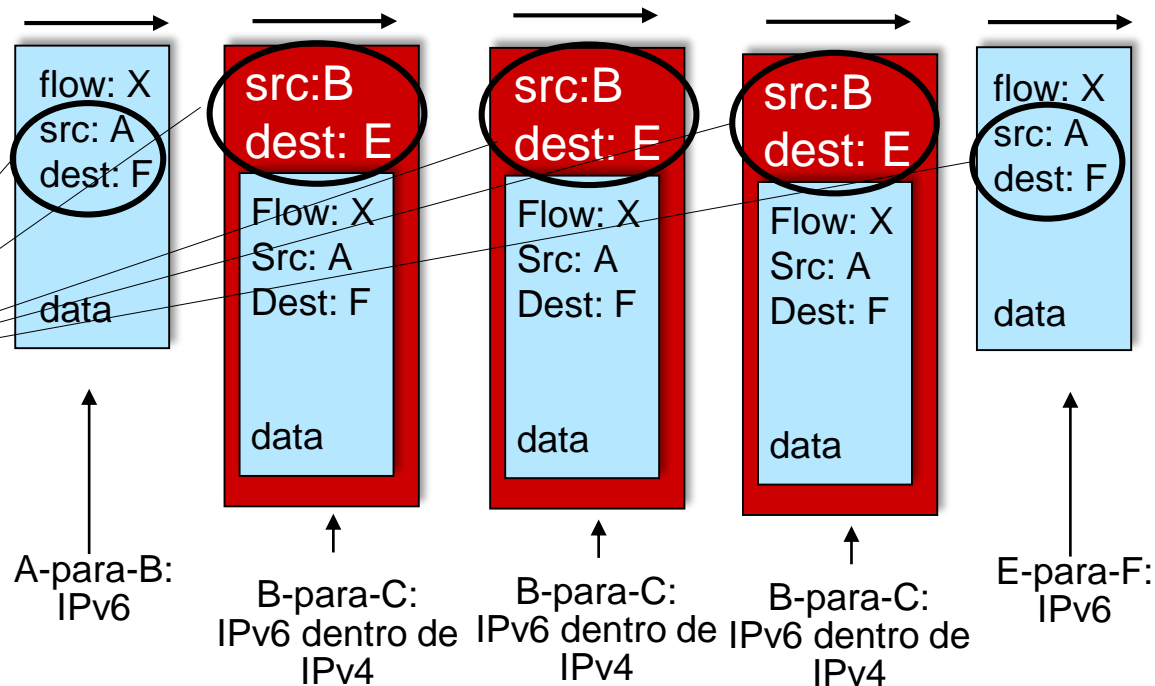
visão lógica:



visão física:



Observe os
endereços de
origem e destino!

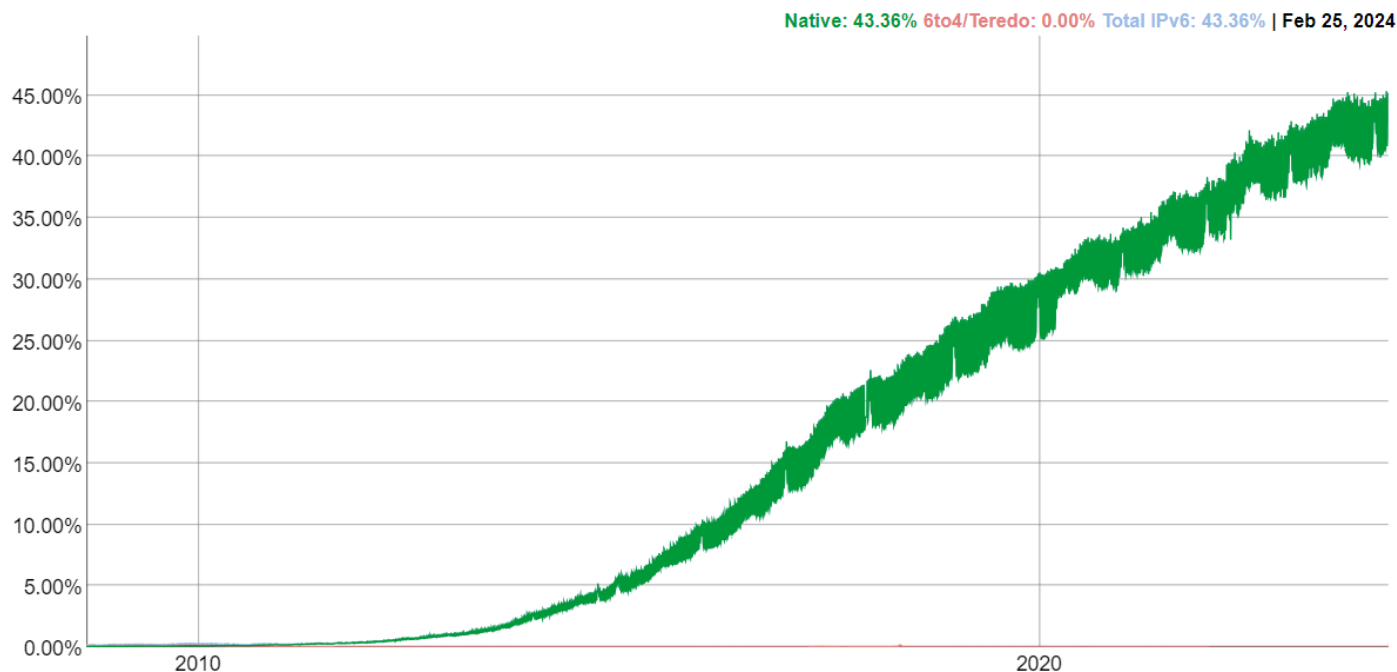


IPv6: adoção

- Google: ~40% de clientes acessam serviços via IPv6 (2023)
- NIST: 1/3 de todos os domínios do governo dos EUA são compatíveis com IPv6

IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



IPv6: adoção

- Google: ~40% de clientes acessam serviços via IPv6 (2023)
- NIST: 1/3 de todos os domínios do governo dos EUA são compatíveis com IPv6
- Tempo de instalação/uso longo (longo!):
 - 28 anos e contando!
 - Pense nas mudanças em nível de aplicação nos últimos 28 anos: WWW, mídia social, streaming de mídia, gaming, telepresença, ...
 - Por quê?

Unidade 4

Camada de Rede

Baseado nos slides elaborados por J. F. Kurose e K. W. Ross

Perguntas?

