Aula 17 - NAT, ICMP e IPv6

Diego Passos

Universidade Federal Fluminense

Redes de Computadores I

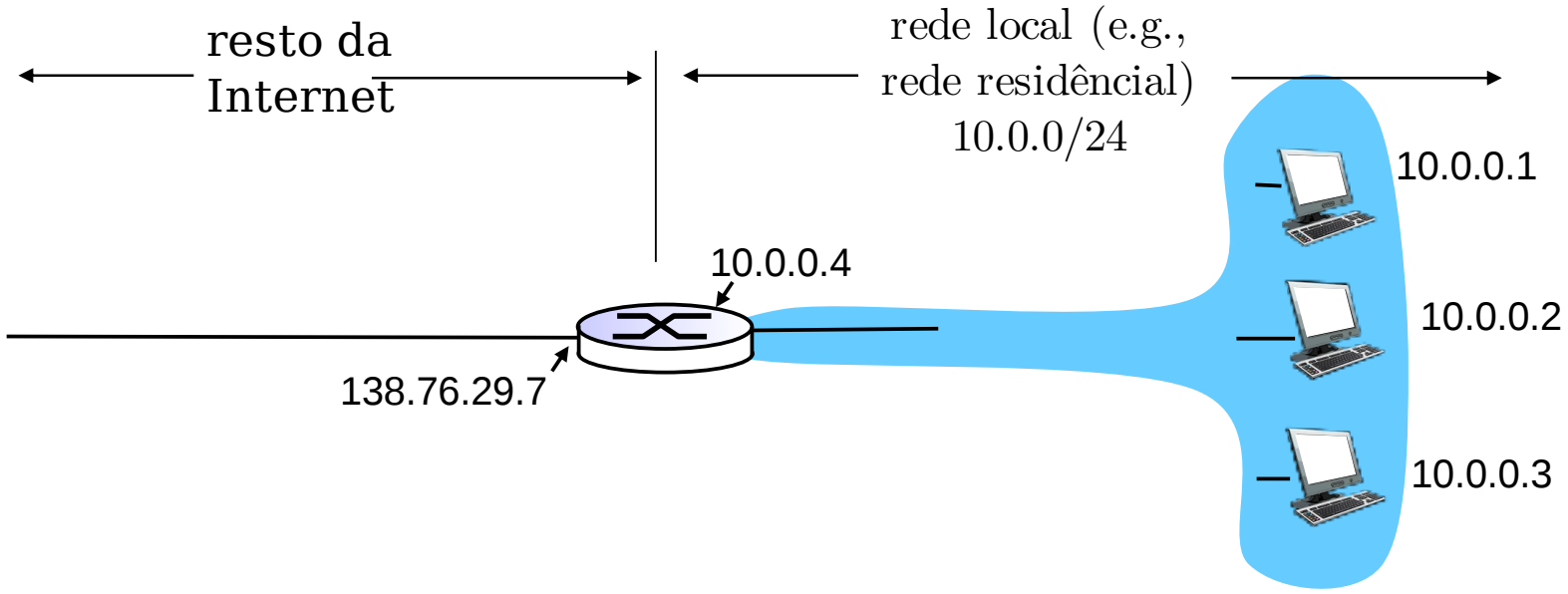
Material adaptado a partir dos slides originais de J.F Kurose and K.W. Ross.

Revisão da Última Aula...

- **Protocolos da Camada de Rede:**
  - Vários contribuem.
  - Protocolos de roteamento.
  - IP.
  - ICMP.
- **Protocolo IP:**
  - Define convenções.
  - Formato de datagrama.
  - Endereçamento.
- **Datagrama IP:**
  - Checksum apenas do cabeçalho.
  - Campo de opções, tamanho variável.
  - TTL (*time-to-live*).
- **Fragmentação:**
  - Quebrar datagramas grandes.
  - Adequa a limitações de cada enlace.
  - **Remontados apenas no destinatário**.
- **Endereçamento IP:**
  - 32 bits.
  - **Associados a interfaces**.
  - **Prefixo identifica a sub-rede**.
  - CIDR, máscara de sub-rede.
- **DHCP:**
  - Protocolo de auto-configuração.
  - Atribuição dinâmica de endereços IP.
  - **Roteador de primeiro salto.**
  - E mais configurações.
  - Cliente-servidor.
  - Roda sobre UDP.
  - Mensagens em ***broadcast***.
- **Endereçamento hierárquico:**
  - Sub-redes são divididas.
  - Novas sub-redes menores.
  - Simplifica anúncio de rotas.

NAT

NAT: *Network Address Translation*



- **Todos** os datagramas **deixando** a rede local possuem o mesmo único endereço de origem: 138.76.29.7.
  - Diferenciação através do **número de porta de origem**.
- Datagramas com origem ou destino nesta rede possuem endereços de origem, destino da sub-rede 10.0.0/24.

NAT: Motivação

- Rede local pode utilizar um único endereço, do ponto de vista do mundo externo.
  - Não é necessária uma faixa de endereços do ISP: um único endereço IP para todos os dispositivos.
  - Pode-se alterar os endereços dos dispositivos locais sem notificação ao mundo externo.
  - Pode-se mudar de ISP sem que os endereços dos dispositivos locais sejam alterados.
  - Dispositivos dentro da rede local não são explicitamente endereçáveis, visíveis ao mundo externo.
    - Um (pequeno) benefício de segurança.
- NAT consegue lidar com a **escassez de endereços IPv4**.

NAT: Implementação

- Um roteador que realiza NAT precisa:
  - **Datagramas que saem: substituir** `(IP de origem, porta de origem)` de cada datagrama para `(IP do roteador, nova porta de origem)`.
    - Nó remoto respoderá utilizando `(IP roteador, nova porta de origem)` como destino.
  - **Armazenar (na tabela NAT)** todo mapeamento feito entre `(IP de origem, porta de origem)` e `(IP roteador, nova porta de origem)`.
  - **Datagramas que chegam: substituir** `(IP roteador, nova porta de origem)` nos campos de destino do pacote por `(IP de origem, porta de origem)` armazenado na tabela NAT.

NAT: Exemplo

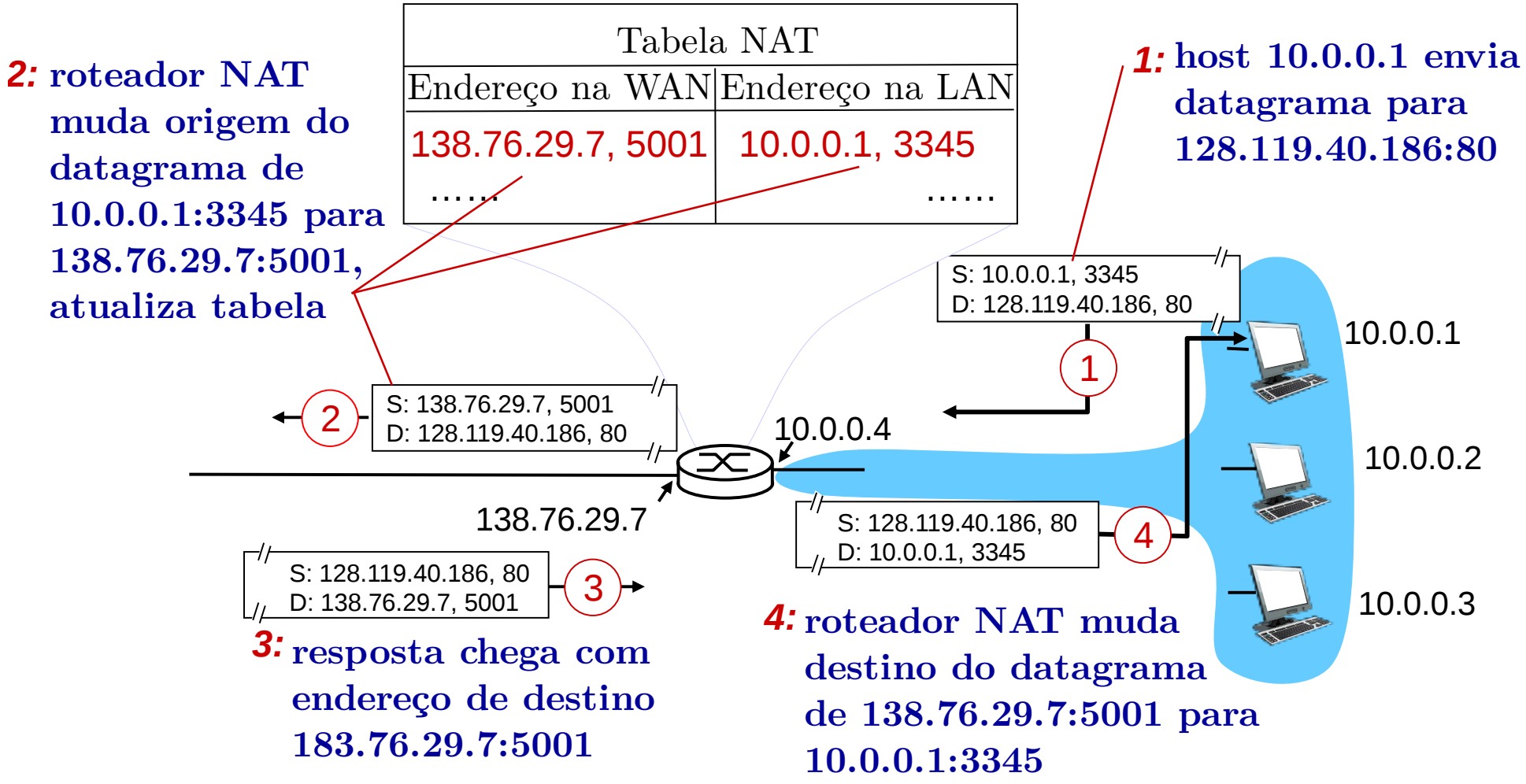


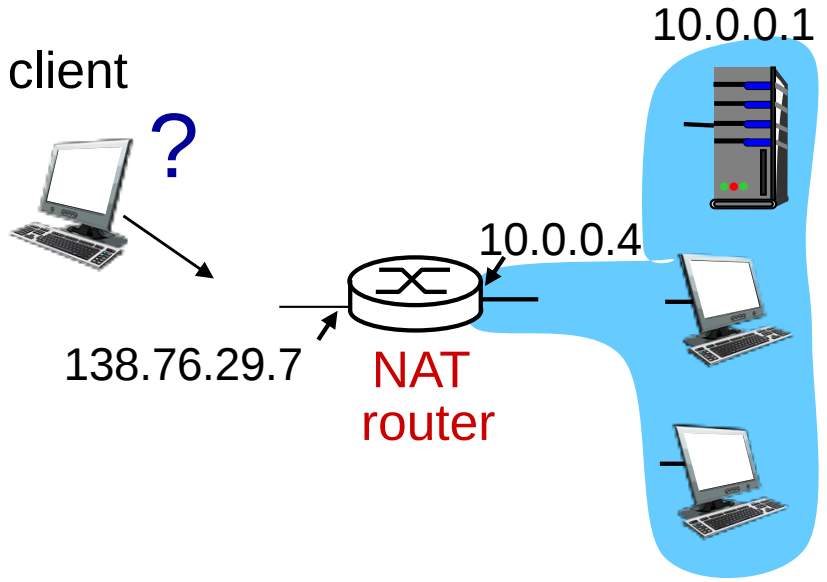
Tabela NAT
Endereço na WAN
Endereço na LAN
138.76.29.7, 5001
10.0.0.1, 3345
.....
.....
2: roteador NAT muda origem do datagrama de 10.0.0.1:3345 para 138.76.29.7:5001, atualiza tabela
1: host 10.0.0.1 envia datagrama para 128.119.40.186:80
S: 10.0.0.1, 3345
D: 128.119.40.186, 80
1
2
S: 138.76.29.7, 5001
D: 128.119.40.186, 80
10.0.0.4
138.76.29.7
10.0.0.1
10.0.0.2
10.0.0.3
S: 128.119.40.186, 80
D: 10.0.0.1, 3345
4
S: 128.119.40.186, 80
D: 138.76.29.7, 5001
3
3: resposta chega com endereço de destino 183.76.29.7:5001
4: roteador NAT muda destino do datagrama de 138.76.29.7:5001 para 10.0.0.1:3345

NAT: Análise

- Campo de número de porta: 16 bits.
  - 65000 conexões simultâneas usando um único endereço IP!
- NAT é controverso:
  - Roteadores só deveriam processar até a camada 3 (camada de rede).
  - NAT viola o argumento fim-a-fim.
    - Muitas vezes, o **NAT precisa ser levado em consideração por projetistas de aplicações**, *e.g.*, aplicações P2P.
  - Escassez de endereços deve ser resolvida pela adoção do IPv6.

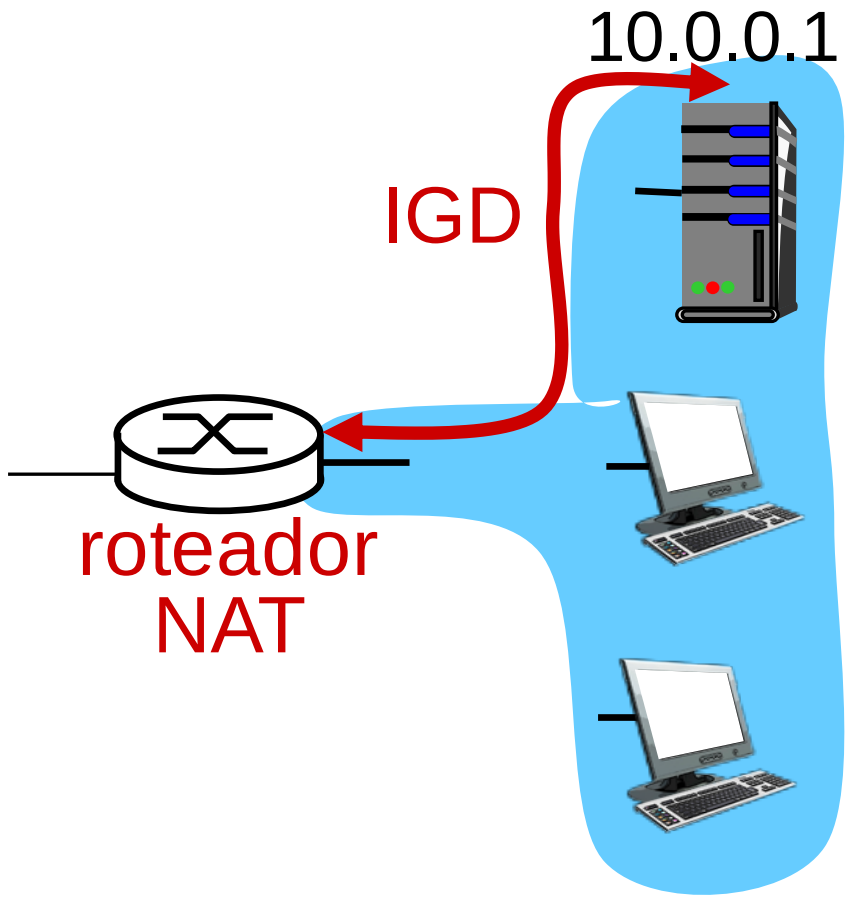
NAT *Traversal* (I)

- Cliente quer se conectar ao servidor com endereço 10.0.0.1.
  - Endereço 10.0.0.1 local para a LAN (cliente não pode usá-lo como endereço de destino).
  - Apenas um endereço visível externamente: 138.76.29.7.
- **Solução 1:** configurar NAT estaticamente para encaminhar conexões que chegam para uma dada porta para o servidor.
  - *e.g.*, `(138.76.29.7, porta 2500)` sempre é traduzido (e encaminhado) para `(10.0.0.1, porta 25000)`.



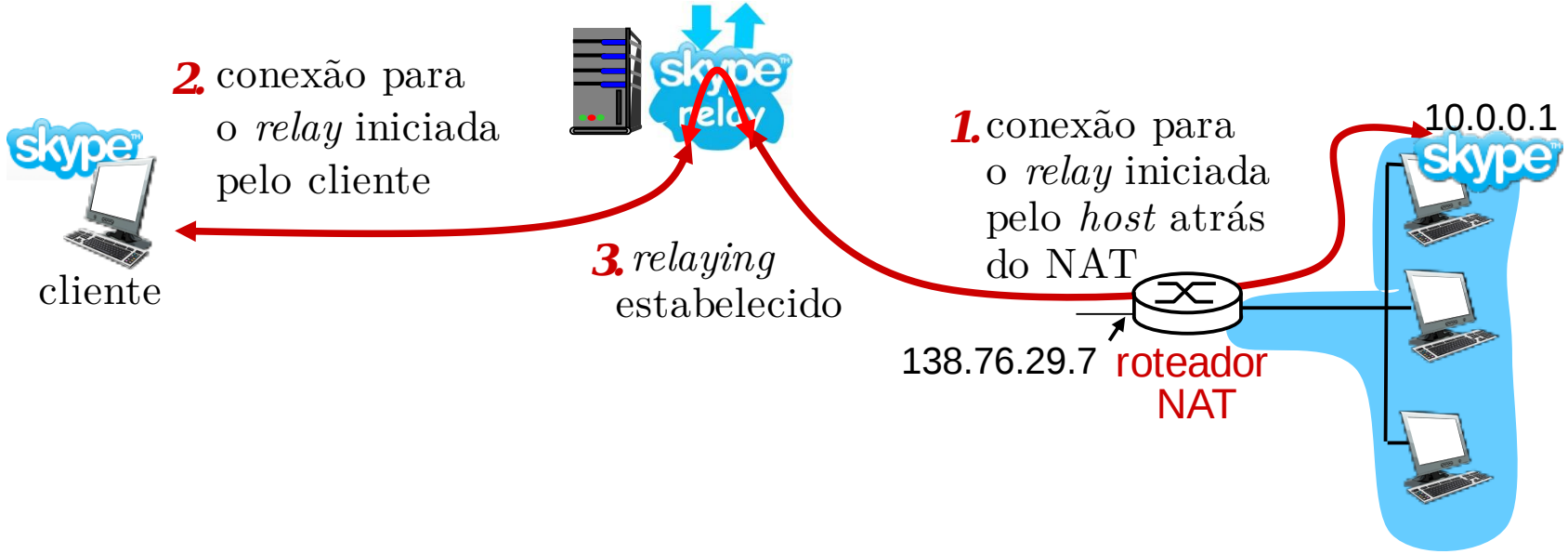
NAT *Traversal* (II)

- **Solução 2:** *Internet Gateway Device Protocol* (IGD).
  - Parte do *Universal Plug and Play* (UPnP).
- Permite que *host* atrás de NAT:
  - Aprenda endereço IP público (138.76.29.7).
  - Adicione/remova mapeamentos de porta (com tempos de *lease*).
- *i.e.*, automatizar configuração estática dos mapeamentos do NAT.



NAT *Traversal* (III)

- **Solução 3:** *relaying* (usado, por exemplo, no Skype).
  - Cliente atrás do NAT estabelece conexão com *host* intermediário.
  - Cliente externo se conecta ao mesmo *host* intermediário.
  - *Host* intermediário (*relay*) faz a ponte entre pacotes das duas conexões.



ICMP

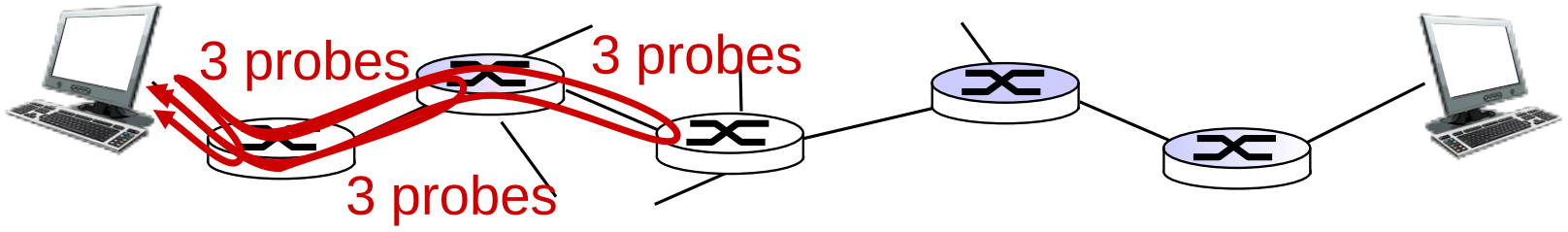
ICMP: *Internet Control Message Protocol*

- Usado por *hosts* e roteadores para comunicar informações no nível de rede.
  - Reportar erros: *host*, rede, porta, protocolo inalcançáveis.
  - *Echo request/reply*: usado pelo utilitário `ping`.
- Protocolo de camada de rede, mas "sobre o IP":
  - Mensagens ICMP transportadas em datagramas IP.
- **Mensagem ICMP:** tipo, código, além dos primeiros 8 bytes do datagrama IP que causaram o erro.

Tipo	Código	Descrição
0	0	*echo reply*
3	0	Rede de destino inalcançável
3	1	*Host* de destino inalcançável
3	2	Protocolo de destino inalcançável
3	3	Porta de destino inalcançável
3	6	Rede de destino desconhecida
3	7	*Host* de destino desconhecido
4	0	*Source quench* (controle de congestionamento, não usada)
8	0	*echo request*
9	0	anúncio de rota
10	0	descoberta de rota
11	0	TTL expirado
12	0	Cabeçalho IP com erros

Traceroute e ICMP

- Origem envia série de segmentos UDP para o destino.
  - Primeiro com TTL = 1.
  - Segundo com TTL = 2, etc.
  - Utiliza porta de destino pouco provável.
- Quando *n-ésimo* conjunto de datagramas chega ao *n-ésimo* roteador:
  - TTL expira, roteador descarta datagrama.
  - Envia mensagem ICMP reportando erro à origem (tipo 11, código 0).
  - Mensagem ICMP inclui nome e endereço IP do roteador.
- Quando mensagem ICMP chega, origem registra o RTT.
- **Critério de parada:**
  - Segmento UDP eventualmente chega ao destinatário.
  - Destinatário envia mensagem ICMP do tipo "porta inalcançável" (tipo 3, código 3).
  - Origem para.



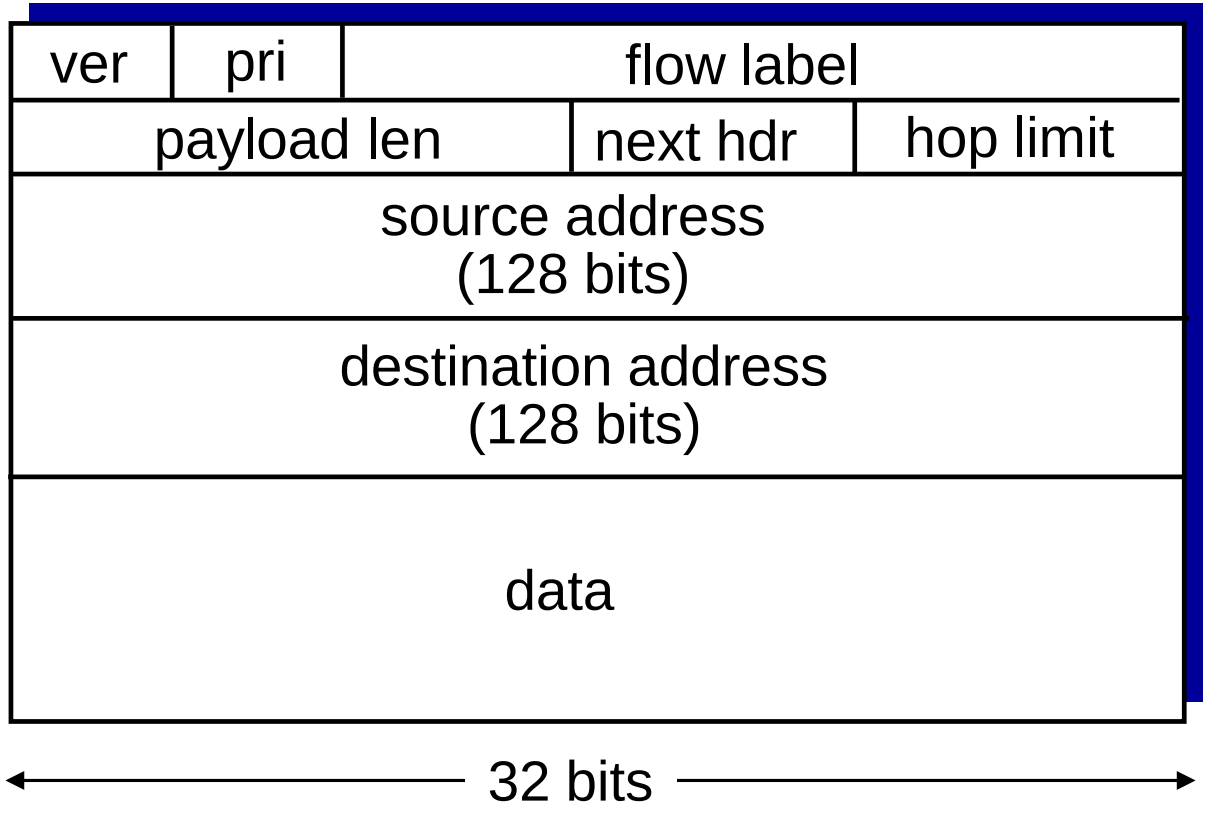
IPv6

IPv6: Motivação

- **Motivação inicial:** espaço de endereçamento de 32 bits será esgotado em breve.
  - *i.e.*, todos os endereços serão alocados.
- Motivações adicionais:
  - Formato do cabeçalho facilita e acelera o processamento/encaminhamento.
  - Alterações no cabeçalho para facilitar QoS.
- **Formato do datagrama IPv6**:
  - Cabeçalho de tamanho fixo, com 40 bytes.
  - Não permite fragmentação.

IPv6: Formato do Datagrama

- **pri:** identifica prioridade do datagrama em relação a outros gerados pela mesma origem.
- **flow label:** identifica datagramas pertencentes a um mesmo "fluxo" (conceito de fluxo não é bem definido).
- **next header:** identifica protocolo para a carga útil do pacote.

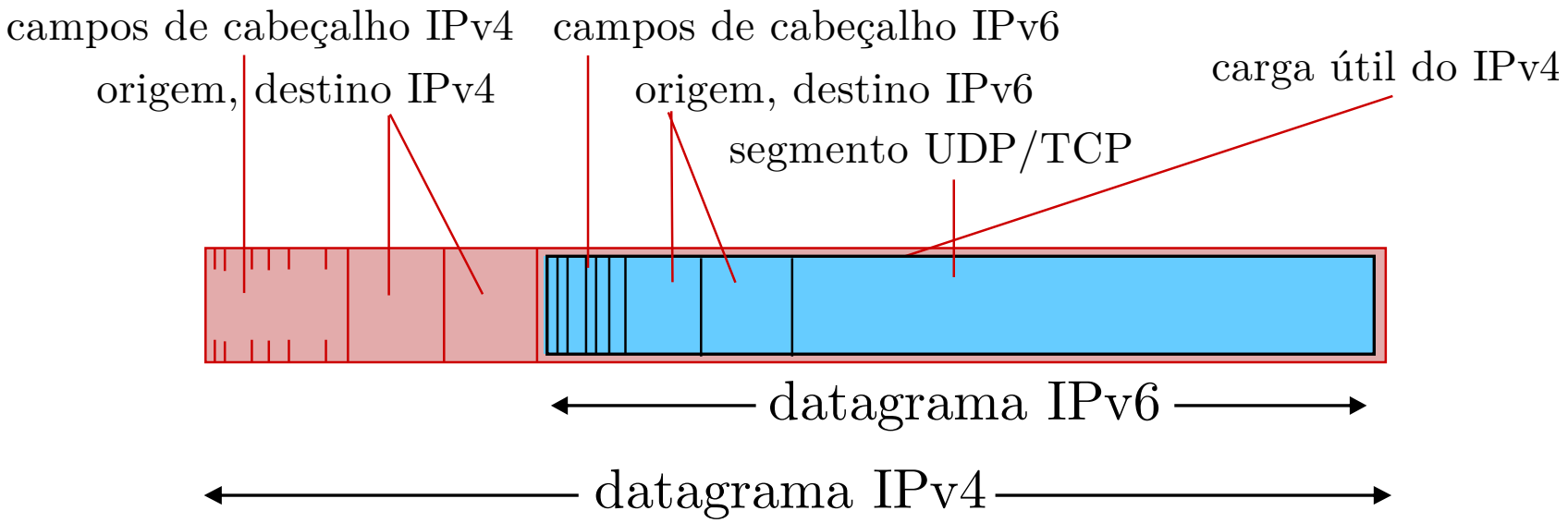


Outras Mudanças em Relação ao IPv4

- **Checksum:** completamente removido para reduzir tempo de processamento em cada salto.
- **Opções:** permitidas, mas **fora do cabeçalho**, indicado pelo valor do campo **next header**.
- **ICMPv6:** nova versão do ICMP.
  - Tipos de mensagem adicionais, *e.g.*, "Pacote Muito Grande".
  - Funções de gerenciamento de grupos multicast.

Transição do IPv4 para o IPv6

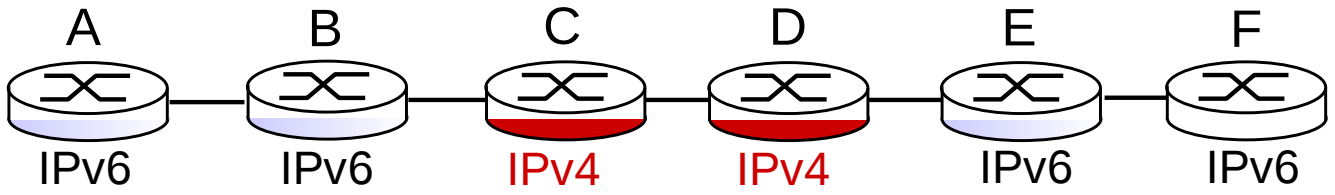
- Impossível atualizar todos os roteadores do mundo simultaneamente.
  - Não existe um “dia oficial de migração”.
  - Como a rede pode operar com roteadores IPv4 e IPv6 misturados?
- **Tunelamento:** datagramas IPv6 carregados como carga útil em datagramas IPv4 encaminhados por roteadores IPv4.



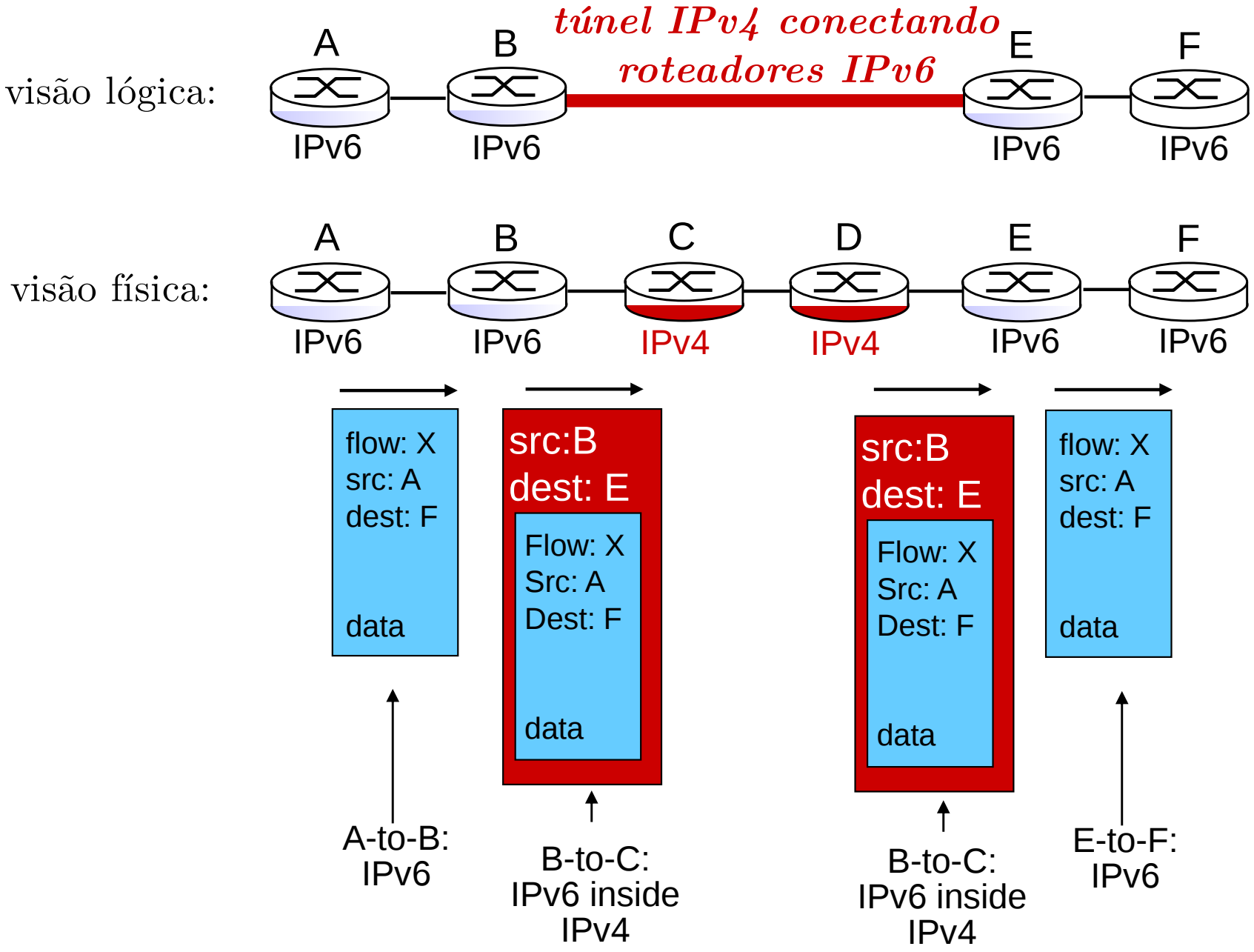
Tunelamento

visão lógica:

visão física:



Tunelamento



IPv6: Adoção

- Estimativas do US National Institute of Standards [2013]:
  - ~3% dos roteadores IP da indústria.
  - ~11% dos roteadores do governo americano.
- **Tempo (muito!) longo para implantação, uso.**
  - 20 anos e contando!
  - Pense nas mudanças no nível de aplicação nos últimos 20 anos: web, facebook, Netflix, ...
  - **Por quê?**

Resumo da Aula...

- **NAT**:
  - Tradução de endereços.
  - Rede local *vs.* rede externa.
  - Endereços privados *vs.* públicos, roteáveis.
  - Pacote sai: IP e porta de origem alterados.
  - Pacote entra: IP e porta de destino são alterados.
  - Tabela NAT: armazana mapeamentos.
- NAT: Motivação.
  - **Escassez de IPs**.
  - Independência dos endereços do ISP.
  - Segurança.
- NAT *Traversal*:
  - Conexão de fora para dentro do NAT.
  - Entradas estáticas na tabela.
  - Protocolo IGD.
  - *Relaying* (aplicação).
- **ICMP:**
  - Gerência do IP.
  - Informações, condições de erro.
  - Diversas tipos de mensagens.
  - Suporte a algumas ferramentas usuais.
- **IPv6: Motivações.**
  - Mais endereços.
  - Menor *overhead* de processamento.
- **IPv6: diferenças**.
  - Cabeçalho fixo.
  - Fragmentação não permitida.
  - Melhor suporte a QoS.
  - ICMPv6.
- **IPv6: Transição.**
  - Gradual, coexistência com IPv4.
  - Solução: tunelamento.

Próxima Aula...

- Iniciaremos a última parte da disciplina: roteamento.
- Na aula que vem:
  - Introdução aos protocolos de roteamento.
  - Classificação dos protocolos.
  - Protocolos baseados em estado de enlace.