



CAMADA DE REDE

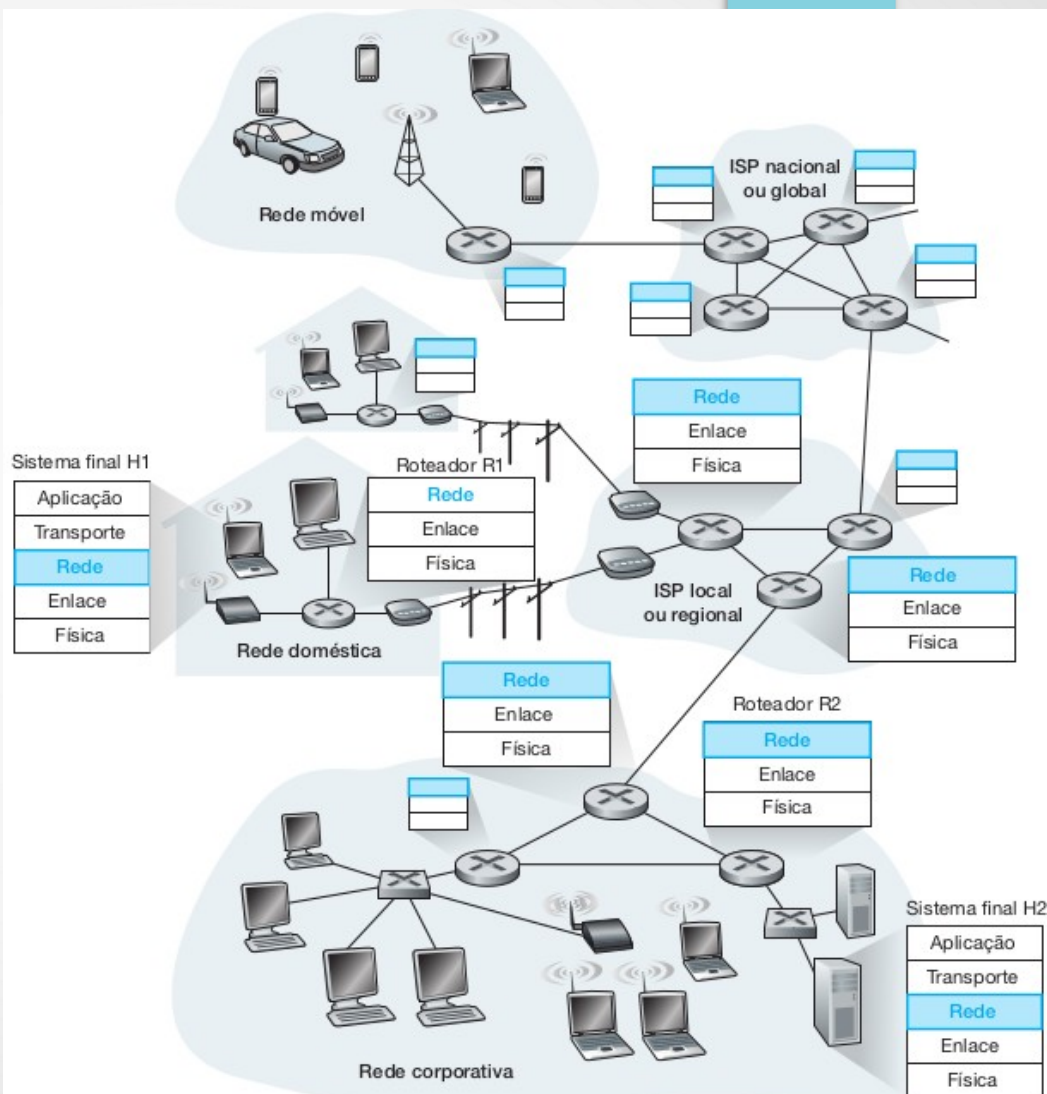
Camada de rede

Objetivos:

- Entender os princípios por trás dos serviços da camada de rede
- **Plano de Dados**
 - modelos de serviço da camada de rede
 - repasse *versus* roteamento
 - como funciona um roteador
 - endereçamento
 - NAT
 - IPv4 e IPv6 (semanas posteriores)
- **Plano de Controle** (semanas posteriores)
 - Principais algoritmos de roteamento
 - ICMP
 - Gerenciamento de rede (semestre que vem!)

Camada de rede

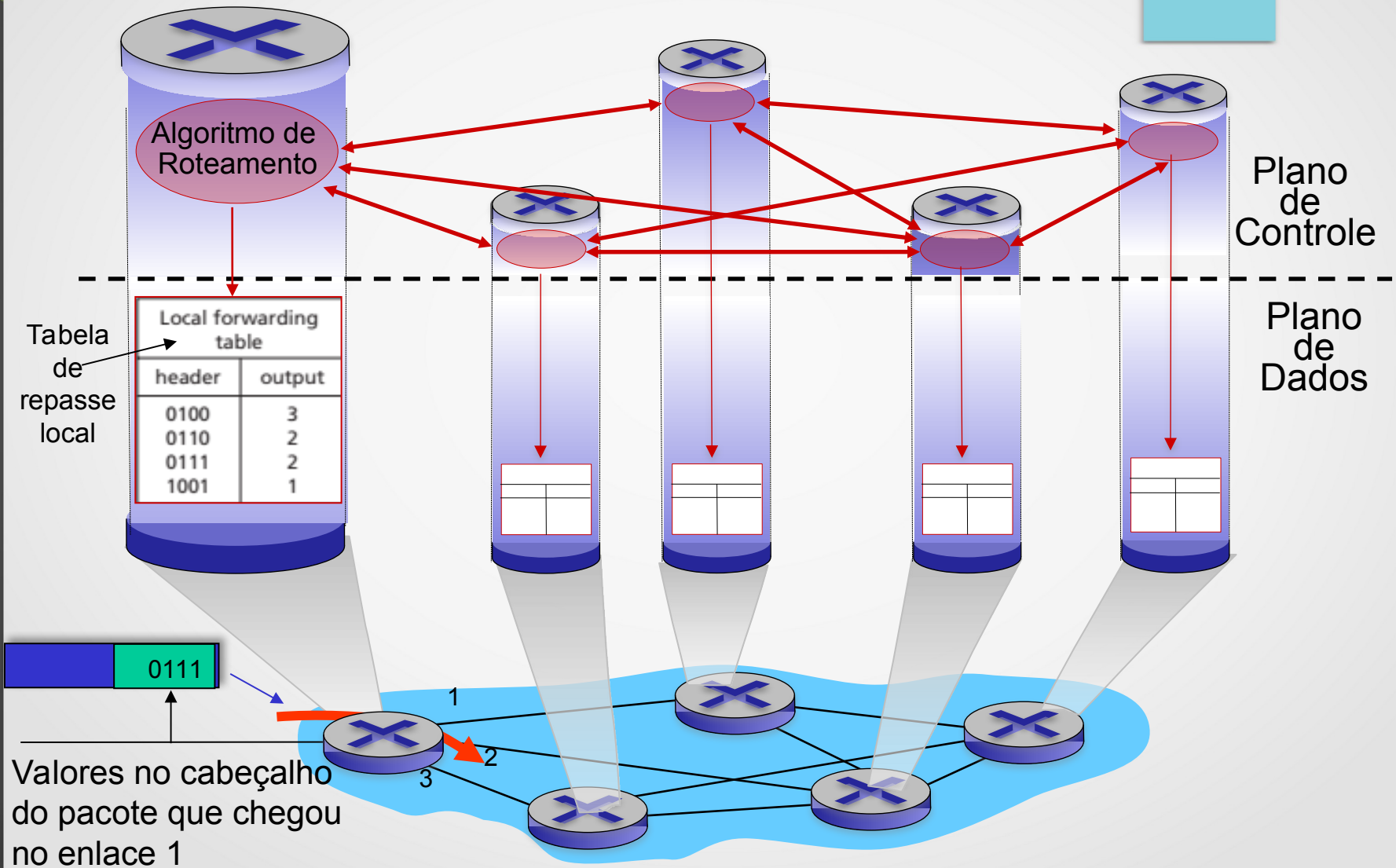
- Envia o segmento recebido da camada de transporte do host emissor para o receptor
- O emissor encapsula segmentos em **datagramas**
- Receptor entrega segmentos à camada de transporte
- **Protocolos da camada de rede** são implementados em *cada host/roteador*
- O roteador examina campos de cabeçalho em todos datagramas IP que passam por ele, movendo de uma interface de entrada para uma de saída.



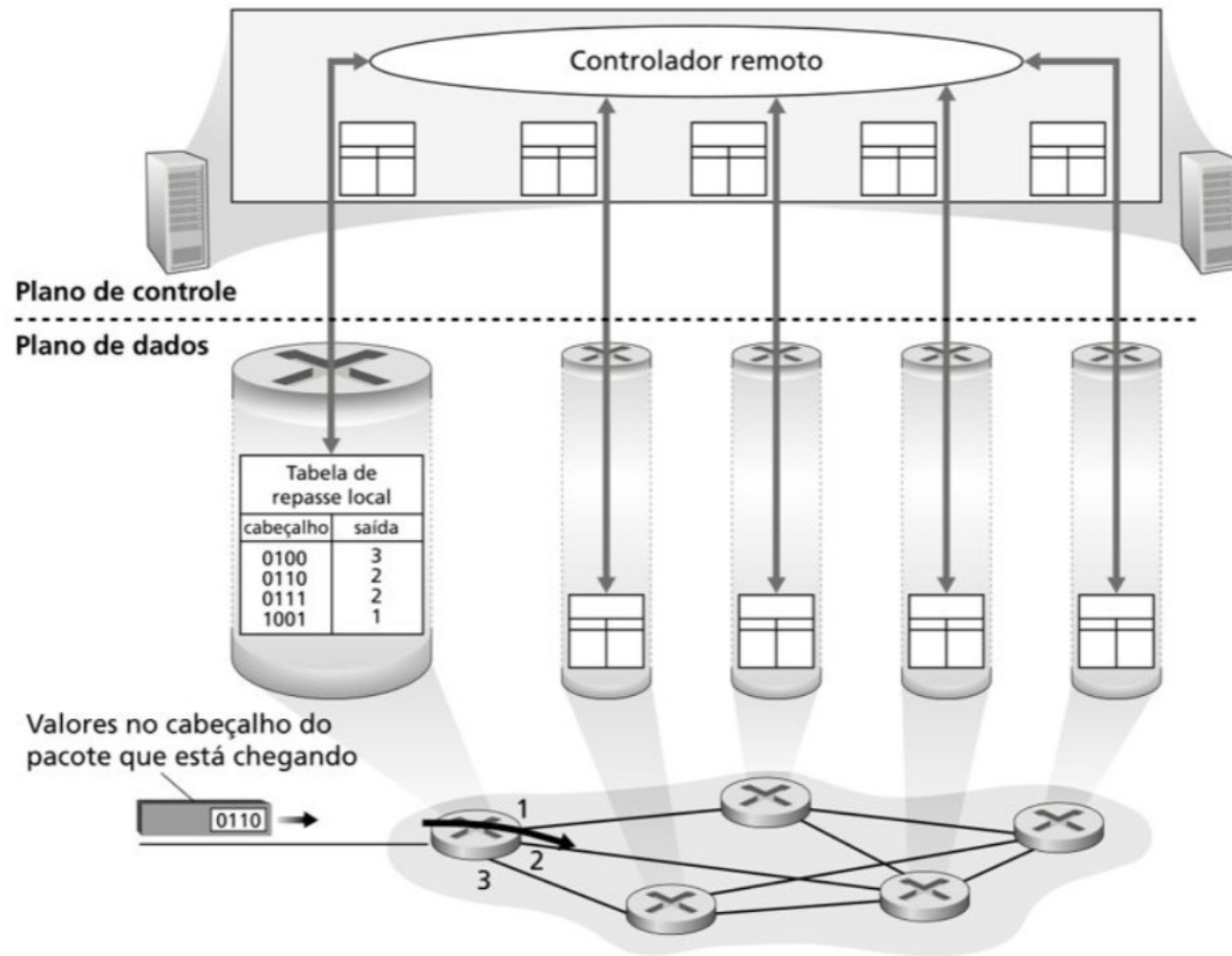
Duas importantes funções da camada de rede: Repasse e Roteamento

- **repasse:** mover datagramas da entrada do roteador p/ a saída apropriada. Executado localmente em cada roteador. **(Plano de dados)**
- **roteamento:** determinar a rota seguida pelos datagramas desde a origem até o destino final, através de todos os roteadores do caminho **(plano de controle)**. Tem 2 abordagens principais:
 - Algoritmo de roteamento tradicional, executado no próprio router.
 - Redes definidas por software (SDN), por meio de servidores.
- *Analogia: roteamento é o processo de planejamento da viagem da origem ao destino, enquanto o repasse é processo de passar por um único cruzamento*
- Cada roteador tem uma tabela de repasse, que tem seus valores definidos pelo algoritmo de roteamento. Cada datagrama que chega ao roteador tem seu cabeçalho examinado e o repasse é feito de acordo com o seu endereço IP e a tabela de repasse.

Interação entre roteamento e repasse tradicional



Interação entre roteamento e repasse em SDN



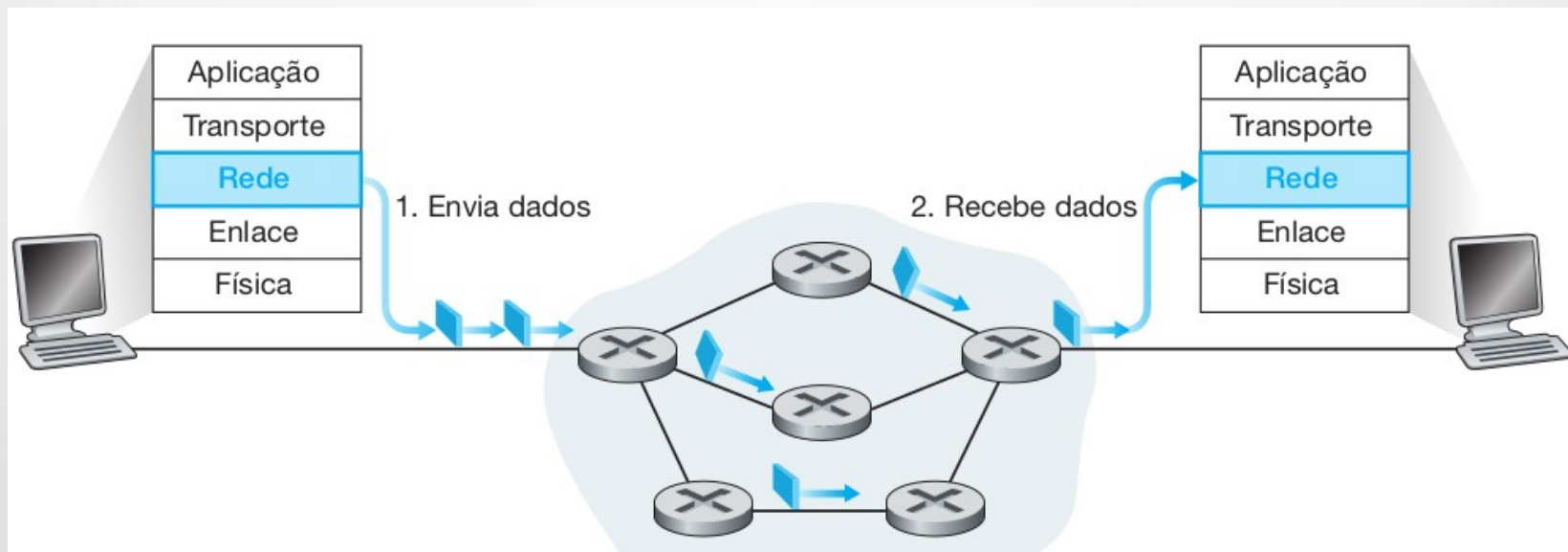
Controlador remoto calcula, e aplica as tabelas de repasse nos routers.

Modelo de serviço de rede

- É possível que a camada de rede implemente alguns serviços:
 - Entrega garantida
 - Entrega garantida com atraso limitado
 - Entrega de pacotes em ordem
 - Largura de banda mínima garantida
 - Segurança, etc.
- Porém, a internet (e a maioria das redes) é uma rede de datagramas, **baseada no melhor esforço**.
 - **Não há nenhum desses serviços na camada de rede**
 - Mas pode haver em outras camadas, se necessário
 - **É funcional se houver dimensionamento adequado**
 - Réplicas e CDN's ajudam a otimizar o acesso.
 - **Por conta desse modelo minimalista a internet foi tão difundida.**

Modelo de serviço: melhor esforço

- Quando um host quer enviar um pacote, ele inclui o endereço de destino final no cabeçalho e envia para a rede.
- O pacote pode passar por uma série de roteadores e cada um utilizará o endereço de destino para repassar o pacote até o destino final.
- Diferentes pacotes da mesma transmissão podem até seguir por caminhos diferentes da origem ao destino.



A camada de rede da Internet

Camada de transporte: TCP, UDP

Protocolos de roteamento

- seleção de caminho
- RIP, OSPF, BGP

Protocolo IP

- convenções de endereçamento
- formato de datagrama
- convenções de manuseio de pacotes

Protocolo ICMP

- comunicação de erro
- “sinalização” de roteador

Tabela de repasse

Camada de rede

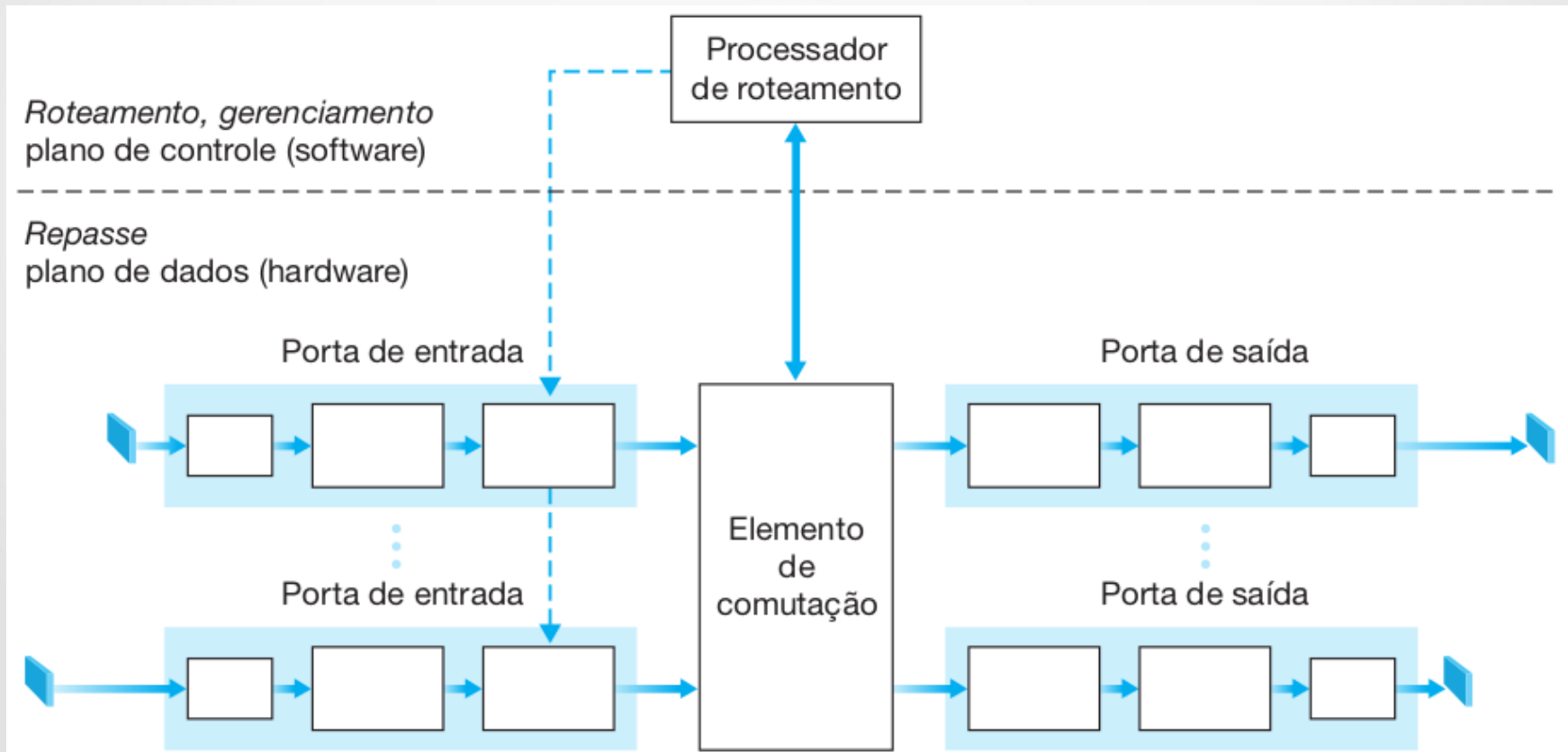
Camada de enlace

Camada física

Visão geral da arquitetura do roteador

Duas funções principais do roteador:

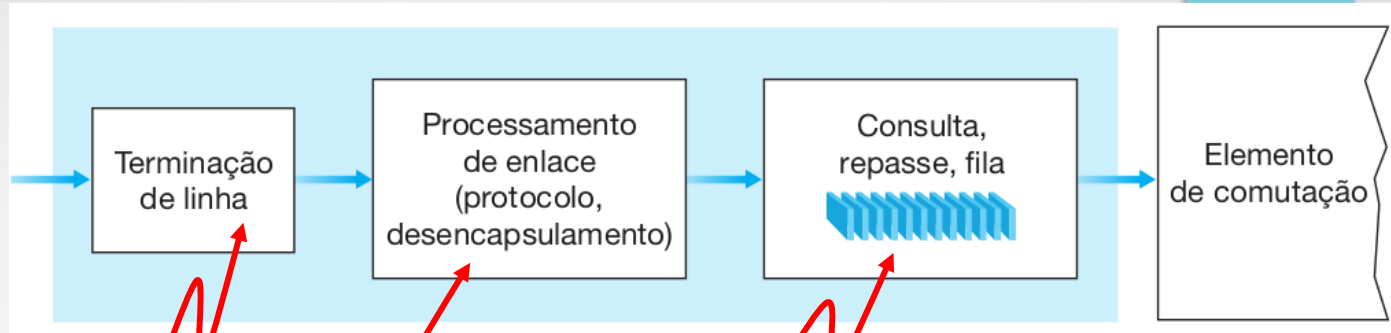
- executar algoritmos/protocolo de roteamento (RIP, OSPF, BGP)
- *repassar* datagramas do enlace de entrada para saída



Visão geral da arquitetura do roteador

- **Porta de entrada** possui funções da camada física e camada de enlace. É na porta de entrada que a tabela de repasse é consultada para determinar a porta de saída utilizada para o pacote.
- **Elemento de comutação** conecta as portas de entrada roteador às suas portas de saída.
- **Porta de saída** armazena os pacotes que foram repassados a ela e os transmite até o enlace de saída, realizando as funções necessárias da camada de enlace e da camada física.
- **Processador de roteamento** executa os protocolos de roteamento, mantém as tabelas de roteamento e as informações de estado do enlace, e calcula a tabela de repasse para o roteador.

Funções da porta de entrada



Camada física:
recepção por bit

Camada de enlace
de dados:
ex: Ethernet

Comutação descentralizada:

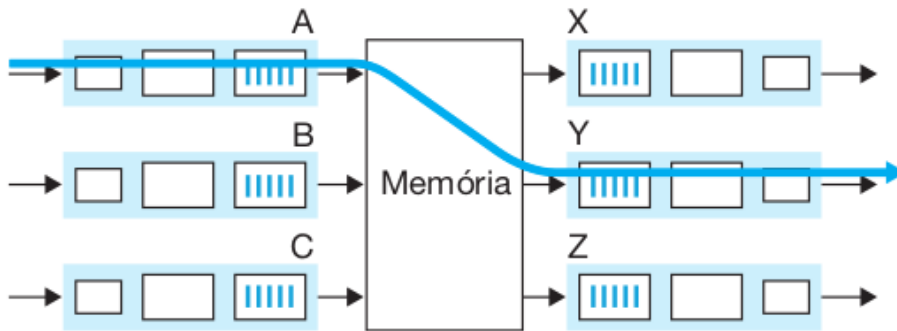
- Verifica o destino do datagrama e escolhe a porta de saída usando cópia tabela de repasse armazenada memória da porta de entrada
- objetivo: realizar o processamento sem chamar o processador e evitar gargalos (velocidade de linha)
- Enfileira se os datagramas chegarem mais rápido que a taxa de repasse

Elemento de comutação – Modos de operação

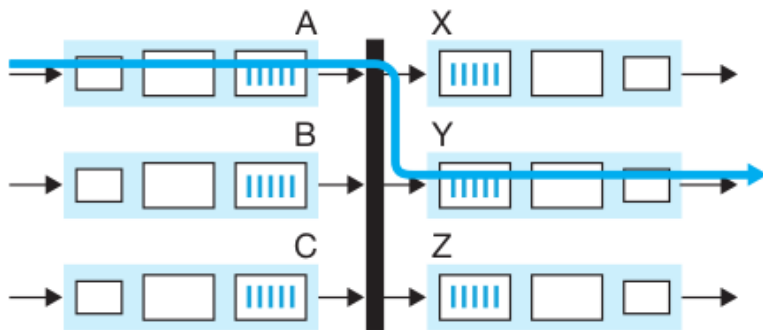
- **Por memória:** 1ª Geração. Ocorre uma sinalização da porta de entrada para o processador, datagrama é copiado para a memória do processador, processador verifica a porta de saída e copia o pacote para o buffer da porta de saída.
- **Por barramento:** datagrama transferido da memória da porta de entrada direto para a memória da porta de saída. Barramento é compartilhado e pode ser um gargalo
- **Por rede de interconexão (crossbar):** Utiliza diversos canais para permitir a transferência de mais datagramas e superar o gargalo do barramento simples.

Elemento de comutação – Modos de operação

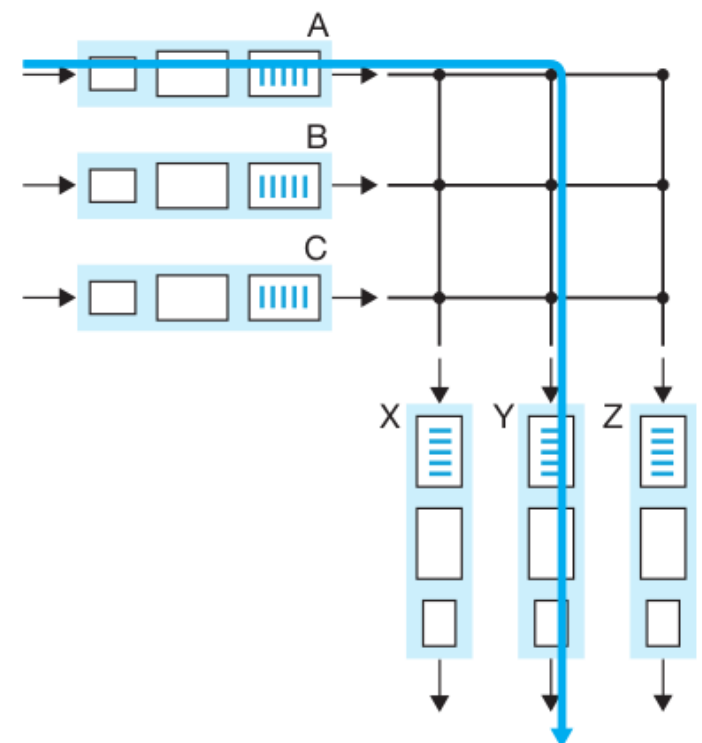
Memória



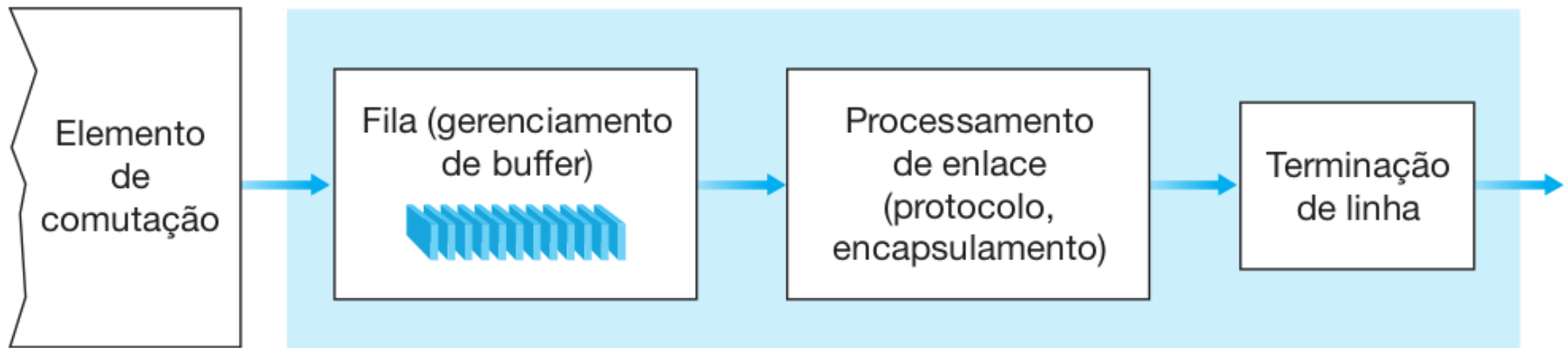
Barramento



Rede de interconexão



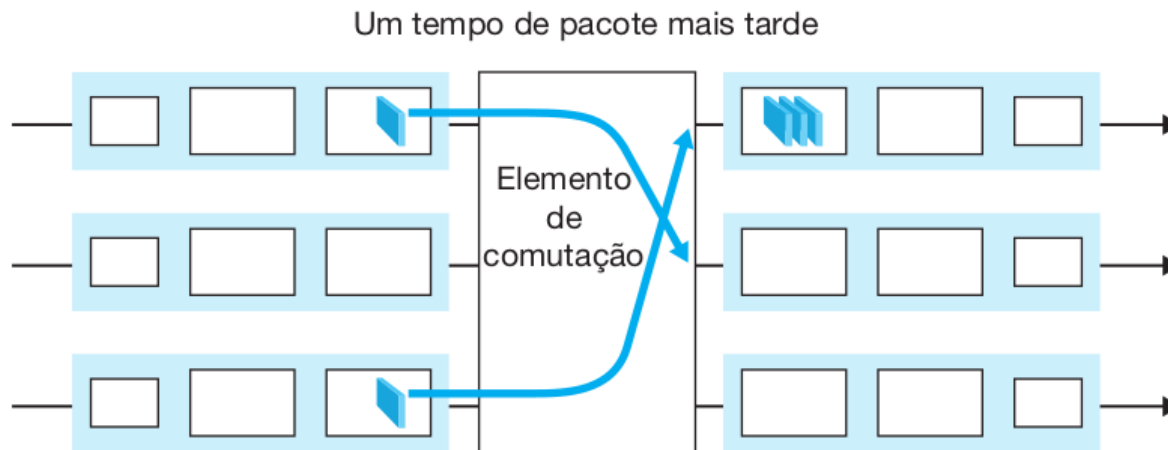
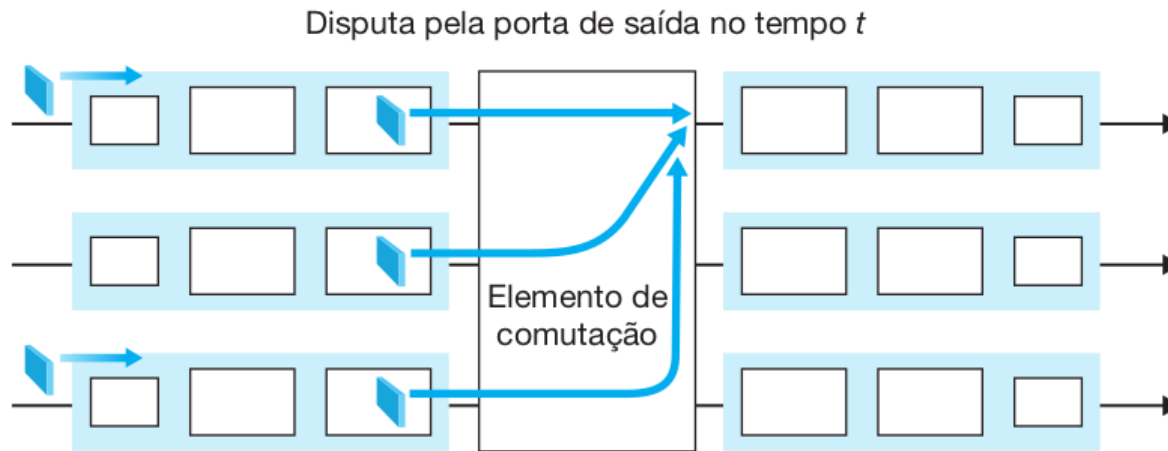
Portas de saída



- **Buffering** exigido quando os pacotes chegam do elemento de comutação mais rápido que a taxa de transmissão
 - *enfileiramento gera atraso e perda de pacotes se esgotar o buffer na porta de saída!*
- **Disciplina de escalonamento** escolhe entre os pacotes enfileirados para transmissão

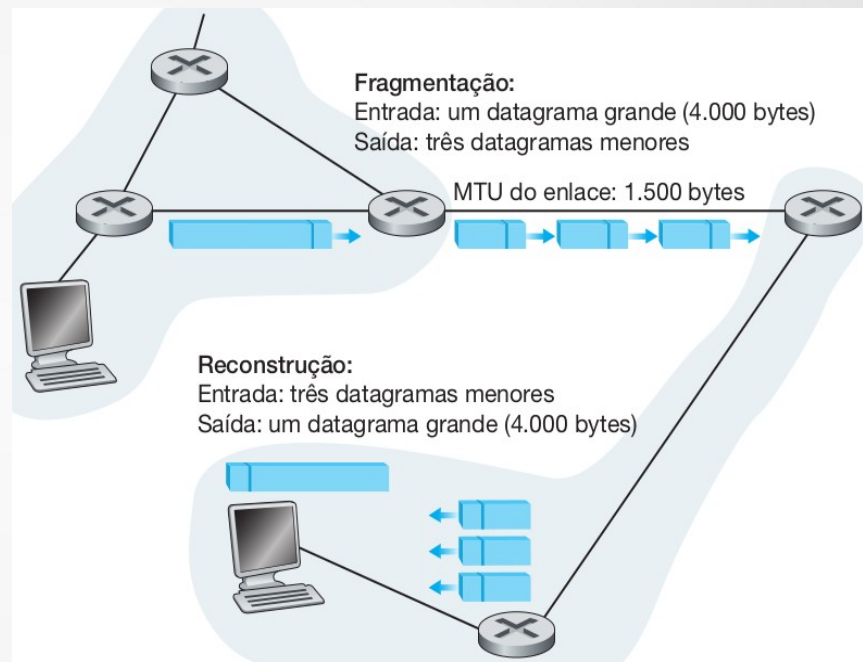
Enfileiramento na porta de saída

FORMAÇÃO DE FILA NA PORTA DE SAÍDA



Fragmentação e reconstrução no IP

- Enlaces possuem **MTU (Maximum Transmission Unit)** - tamanho máximo de transferência de um quadro.
 - Diferentes enlaces e MTU's podem compor o caminho todo.
- No IPv4, um datagrama maior que a MTU é “**fragmentado**”, ou seja, um se torna vários datagramas, e será “reconstruído” no destino
- Porém, **no IPv6** há uma abordagem diferente: **não existe fragmentação**.
- Quando o próximo enlace tem MTU maior que o datagrama, o emissor é informado desse valor através de um pacote ICMPv6 e deve reconfigurar os datagramas no tamanho correto.

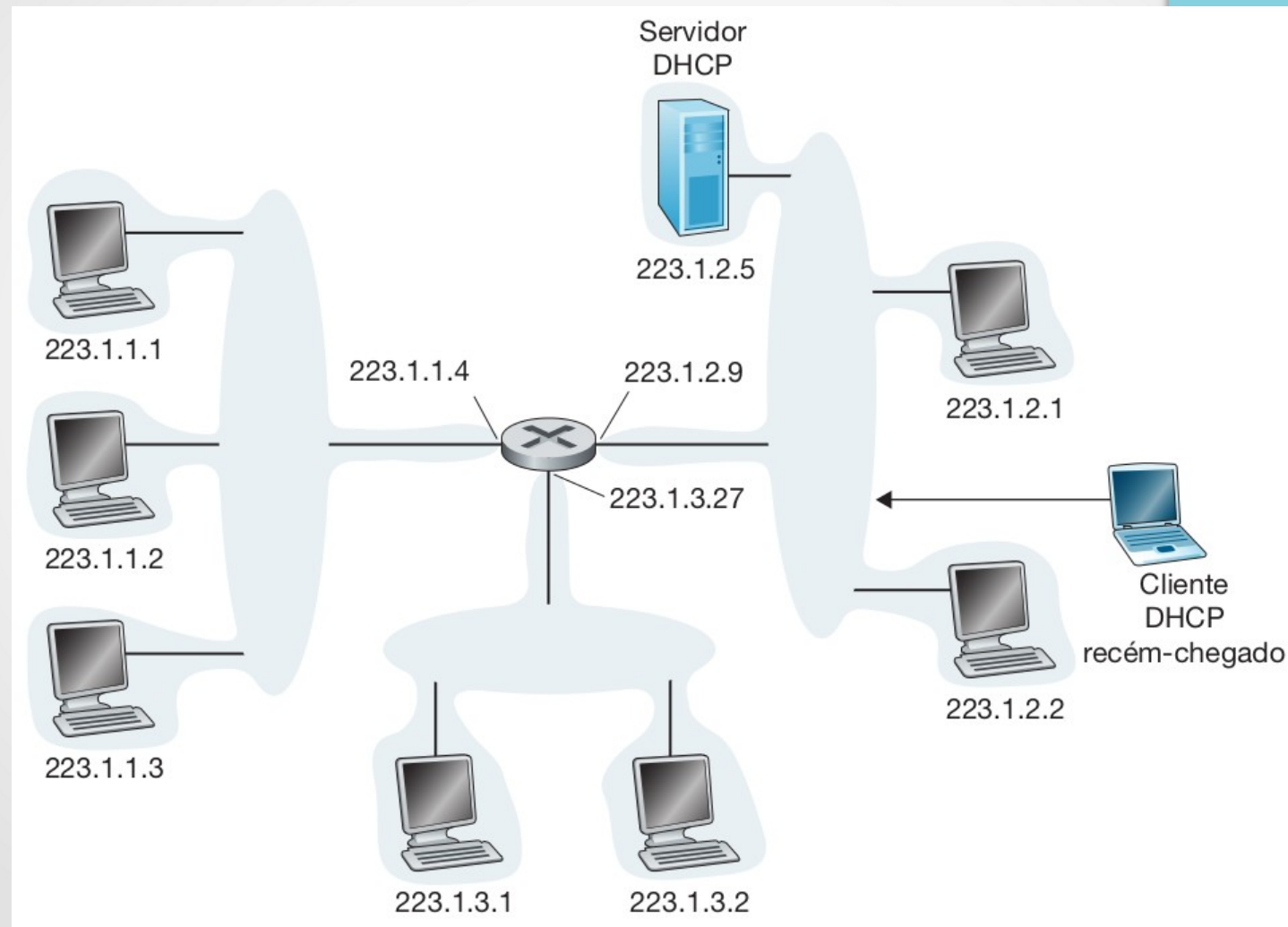


DHCP: Dynamic Host Configuration Protocol

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

- pode renovar seu prazo no endereço utilizado (lease time)
- permite reutilização de endereços (só mantém endereço enquanto conectado e “ligado”)
- aceita usuários móveis que queiram se juntar à rede
- pode fornecer também: gateway, DNS e máscara de sub-rede
- **Visão geral do DHCP:**
 - host envia a msg “DHCP discover” em broadcast [opcional]
 - servidor DHCP responde com msg “DHCP offer” [opcional]
 - host requisita endereço IP com msg “DHCP request”
 - servidor DHCP envia endereço com msg “DHCP ack”

DHCP – cenário cliente/servidor



Servidor DHCP:
223.1.2.5



Cliente recém-chegado



Descoberta DHCP

Origem: 0.0.0.0, 68
Destino: 255.255.255.255, 67
DHCPDISCOVER
Internet: 0.0.0.0
ID transação: 654

Oferta DHCP

Origem: 223.1.2.5, 67
Destino: 255.255.255.255, 68
DHCPOFFER
Internet: 223.1.2.4
ID transação: 654
ID servidor DHCP: 223.1.2.5
Vida útil: 3.600 s

Requisição DHCP

Origem: 0.0.0.0, 68
Destino: 255.255.255.255, 67
DHCPREQUEST
Internet: 223.1.2.4
ID transação: 655
ID servidor DHCP: 223.1.2.5
Vida útil: 3600 s

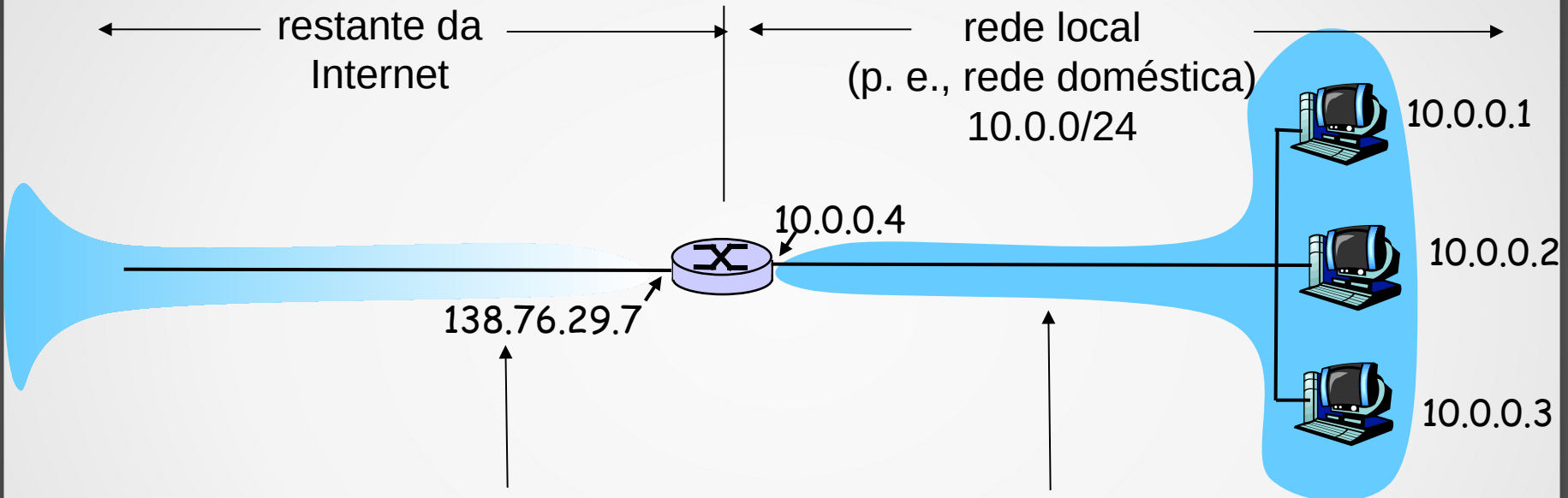
ACK DHCP

Origem: 223.1.2.5, 67
Destino: 255.255.255.255, 68
DHCPACK
Internet: 223.1.2.4
ID transação: 655
ID servidor DHCP: 223.1.2.5
Vida útil: 3.600 s

Tempo

Tempo

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)

Vantagens e desvantagens do uso de NAT

- Campo de número de porta de 16 bits permite mais de 65mil conexões simultâneas com um único endereço no lado da LAN!
- Rede local inteira usa apenas um endereço IP válido para a Internet
- Pode mudar os endereços dos hosts da local sem notificar a Internet
- Pode mudar de ISP sem alterar os endereços os hosts na rede local
- Dispositivos locais não precisam ser explicitamente endereçáveis ou visíveis pela Internet (uma questão de segurança).
- Mas, o NAT é controverso e viola argumento de fim a fim, já que roteadores só deveriam processar até a camada 3
- A possibilidade de NAT deve ser levada em conta pelos projetistas da aplicação, já que pode inviabilizar aplicações P2P.
- Com IPv6 torna-se desnecessário
 - Mas ainda pode ser utilizado

Implementação

Roteador NAT deve:

- *enviando datagramas: substituir* (endereço IP de origem, número da porta) de cada datagrama saindo por (endereço IP da NAT, novo número de porta)
... clientes/servidores remotos responderão usando (endereço IP da NAT, novo número da porta) como endereço de destino
- *lembrar (na tabela de tradução NAT)* de cada par de tradução (endereço IP de origem, número porta) para (endereço IP da NAT, novo número da porta)
- *recebendo datagramas: substituir* (endereço IP da NAT, novo número da porta) nos campos de destino de cada datagrama chegando por (endereço IP origem, número da porta) correspondente, armazenado na tabela NAT

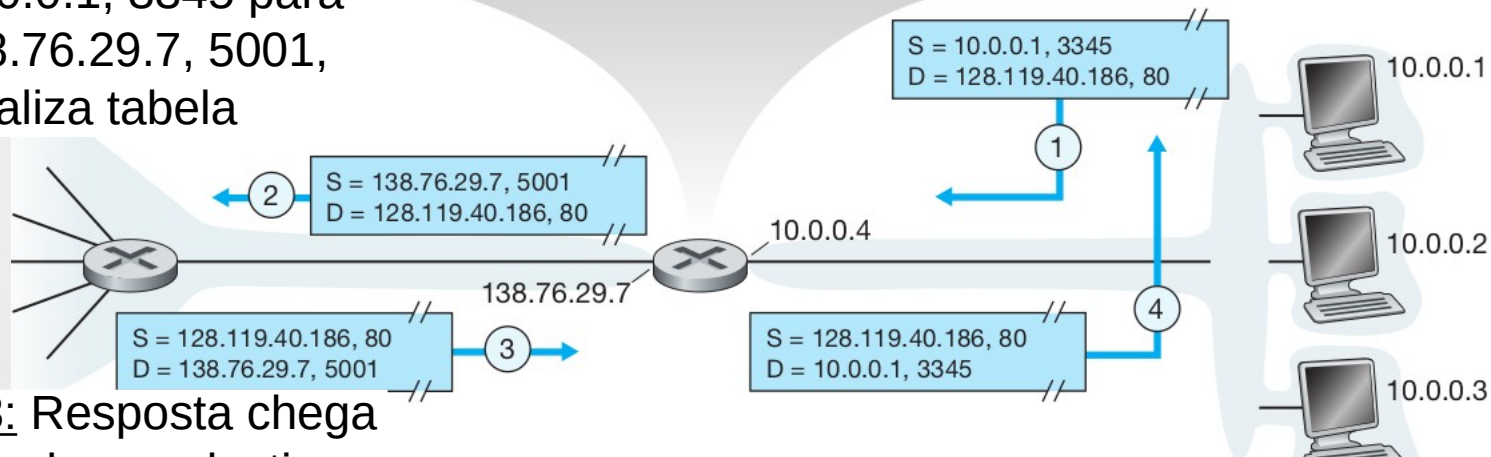
2: roteador NAT muda endereço de origem do datagrama de 10.0.0.1, 3345 para 138.76.29.7, 5001, atualiza tabela

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

1: host 10.0.0.1 envia datagrama para 128.119.40.186, 80

3: Resposta chega endereço destino: 138.76.29.7, 5001

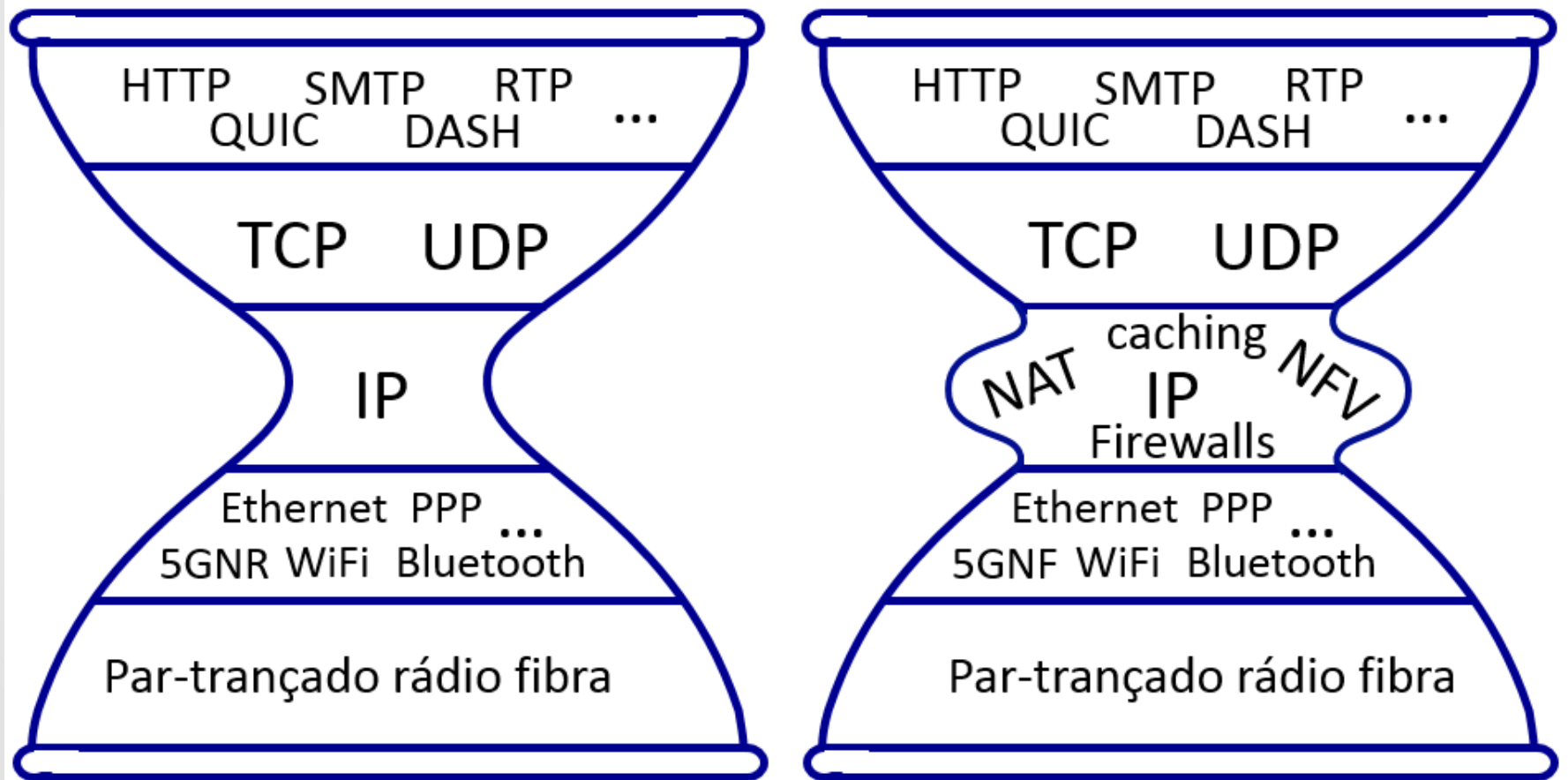
4: roteador NAT muda endereço de destino do datagrama de 138.76.29.7, 5001 para 10.0.0.1, 3345



Middleboxes

- Segundo a RFC 3234, um middlebox é qualquer dispositivo intermediário executando funções não triviais para um roteador IP no caminho de dados entre um host de origem e um host de destino.
- Cada vez mais existem nas redes, modificando os princípios fim a fim da internet, em que a inteligência deveria estar nos hosts.
- Em geral executam:
 - **Tradução NAT**
 - **Serviços de segurança**
 - Firewall, IDS, filtros de e-mail, etc.
 - **Melhoria de desempenho**
 - Cache, CDN, balanceamento de carga, compressão, etc.

O antes e o depois da arquitetura da Internet



ICMP: Internet Control Message Protocol

- usado por hosts e roteadores para comunicar informações em nível de rede
 - relato de erro: host, rede, porta, protocolo inalcançável
 - eco de solicitação/ resposta (usado por ping)
- Está na camada de rede “acima” do IP:
 - mensagens ICMP enviadas em datagramas IP
- **mensagem ICMP:** tipo, código mais primeiros 8 bytes do datagrama IP causando erro

<u>Tipo</u>	<u>Cód.</u>	<u>Descrição</u>
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 rota
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.



Referência:

Cap.4-Camada de rede.

Livro: **Redes de computadores e a Internet** de J.
F Kurose e K. W. Ross, 6ª ed.