

# IPv6

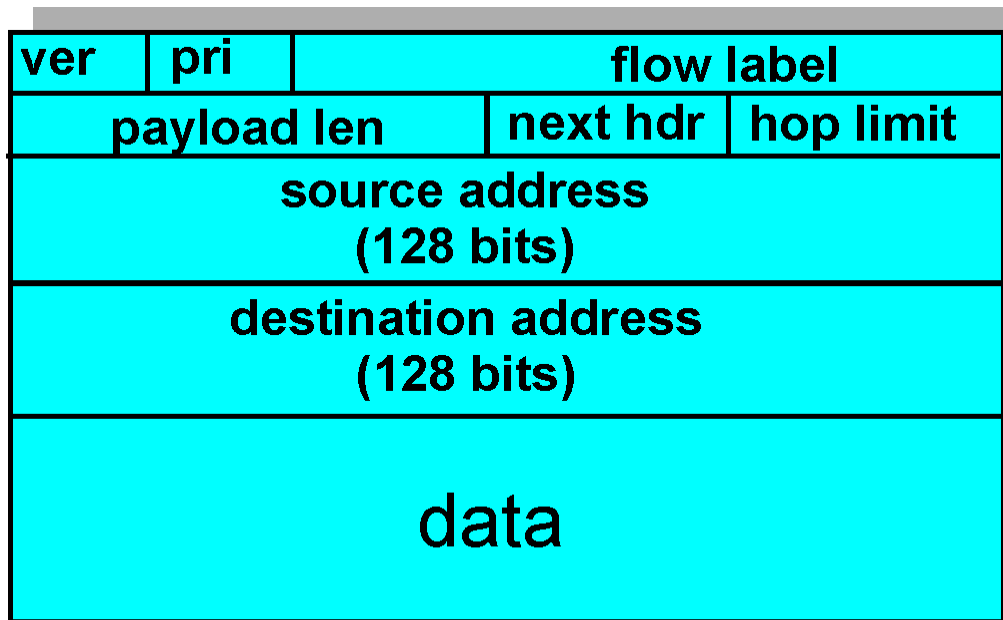
- ❑ **Motivação inicial:** o espaço de endereços de 32-bits brevemente estará completamente alocado.
- ❑ **Motivação adicional:**
  - ✓ melhorar o formato do cabeçalho para permitir maior velocidade de processamento e de transmissão
  - ✓ mudanças no cabeçalho para incorporar mecanismos de controle de QoS (*Quality of Service*).  
*Ex: diferenciação de fluxos de áudio e vídeo, com alta prioridade*
- ❑ **Formato dos datagramas IPv6:**
  - ✓ cabeçalho fixo de 40 bytes
  - ✓ não é permitida a fragmentação

# IPv6: Cabeçalho

*Pri (classe de tráfego):* 8 bits - permite definir/identificar prioridades diferenciadas para vários pacotes dentro de um determinado fluxo de informação (ou a datagramas icmp, por ex)

*Flow Label:* 20 bits - identifica datagramas do mesmo "fluxo."

*Next header:* identifica o protocolo da camada superior (UDP ou TCP)



*payload len:* 16 bits - comprimento da carga útil

*Hop limit (limite de saltos):* 4 bits - qtde de enlaces máxima

← 32 bits →

# Mudanças em relação ao IPv4

- ❑ **Fragmentação:** não é permitida nos roteadores intermediários (somente na fonte e no destino)
  - ✓ *Objetivo: reduzir tempo de processamento*
  - ✓ *Descarta qdo pacote é grande demais e envia msg de erro à origem*
- ❑ **Checksum:** removido inteiramente para reduzir o tempo de processamento em cada roteador (no IPv4 o campo TTL, decrementado em cada roteador, obrigava a recalcular o checksum)
  - ✓ Justificativa: já é realizado tanto na camada de enlace quanto na camada de transporte (redundante)

# Outras mudanças em relação ao IPv4

- ❑ *Opções:* não disponíveis (já existem nas camadas superiores, indicadas pelo campo "Next Header")

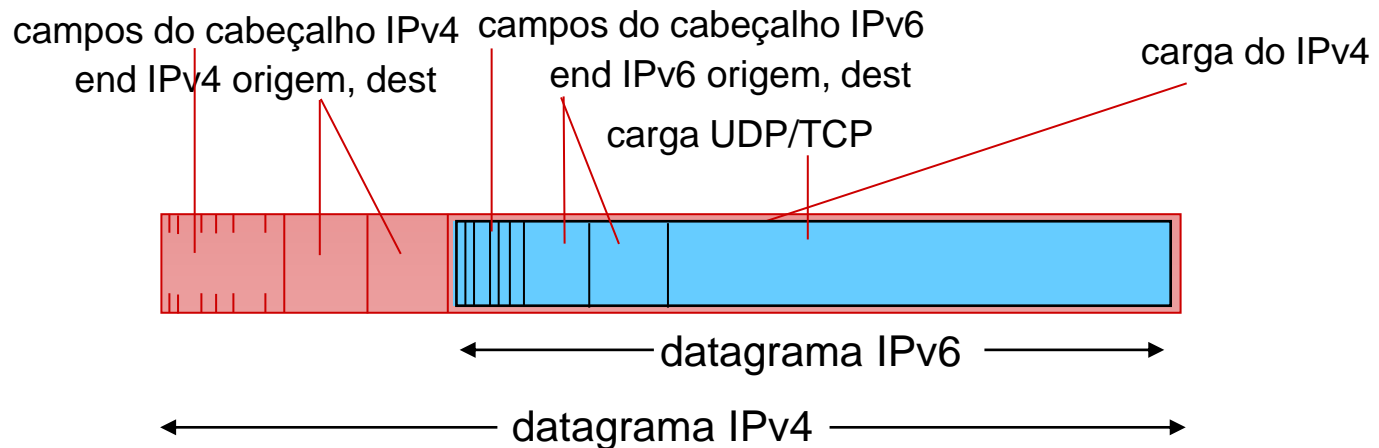
# Transição do IPv4 para IPv6

- O IPv6 pode enviar, rotear e receber datagramas IPv4, enquanto o contrário não é possível
- Nem todos os roteadores poderão ser atualizados simultaneamente
  - não haverá um dia da “mudança geral”
  - *Como a rede irá operar com os dois tipos de datagramas simultaneamente?*
- Abordagem amplamente usada: tunelamento

# Transição do IPv4 para IPv6

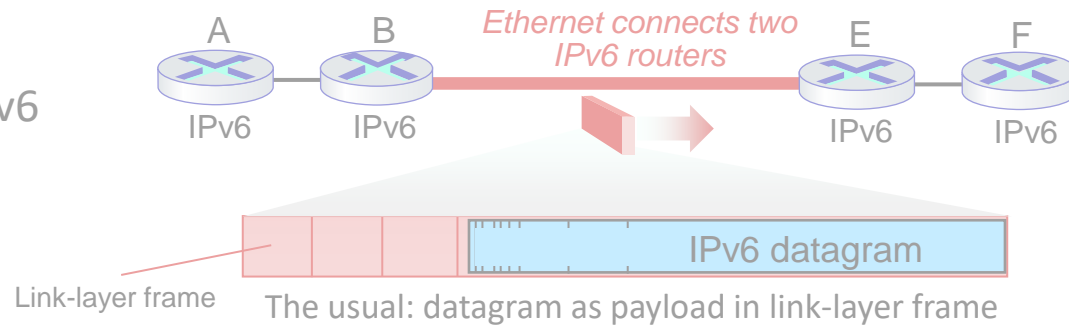
**Tunelamento** - datagrama IPv6 é enviado como carga útil de um datagrama IPv4 entre roteadores IPv4

- Obs:**
1. mudança dos protocolos da cam. de rede (IPv4 para IPv6) - difícil
  - mudança dos protocolos da cam. de aplicação - mais tranquila
  2. tunelamento usado extensivamente em outros contextos (4G/5G)

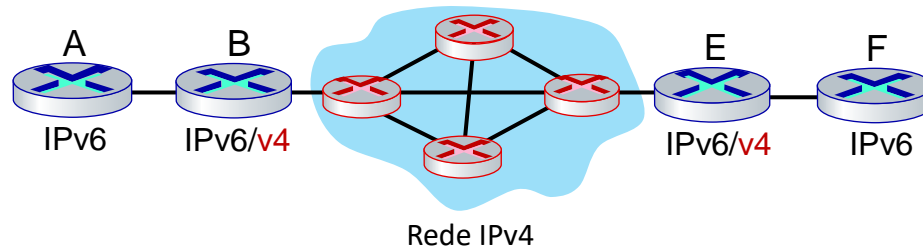


# Tunelamento e encapsulamento

Ethernet  
connecting two IPv6  
routers:

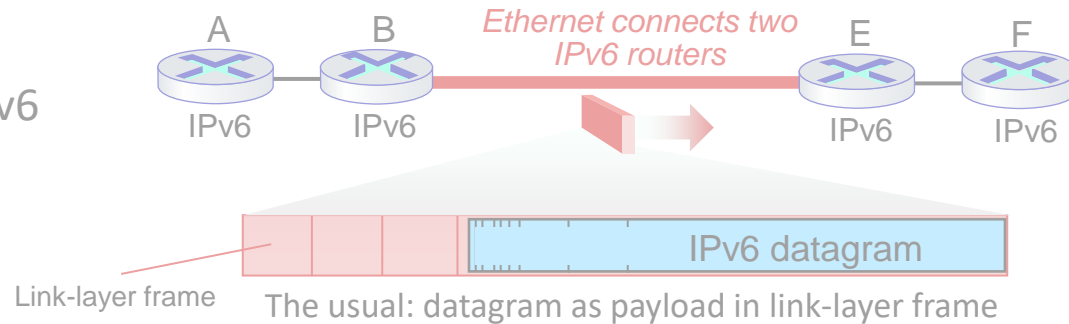


Rede IPv4  
conectando dois  
roteadores IPv6

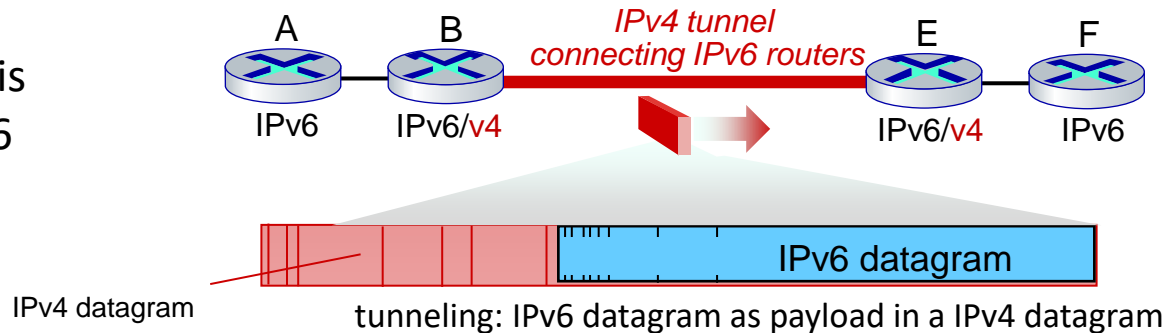


# Tunelamento e encapsulamento

Ethernet  
connecting two IPv6  
routers:



Túnel IPv4  
conectando dois  
roteadores IPv6



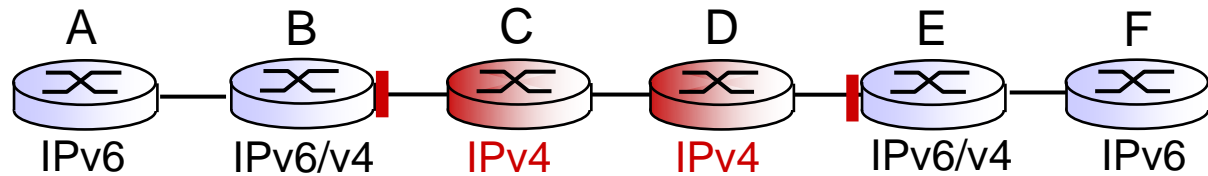


# Túnel

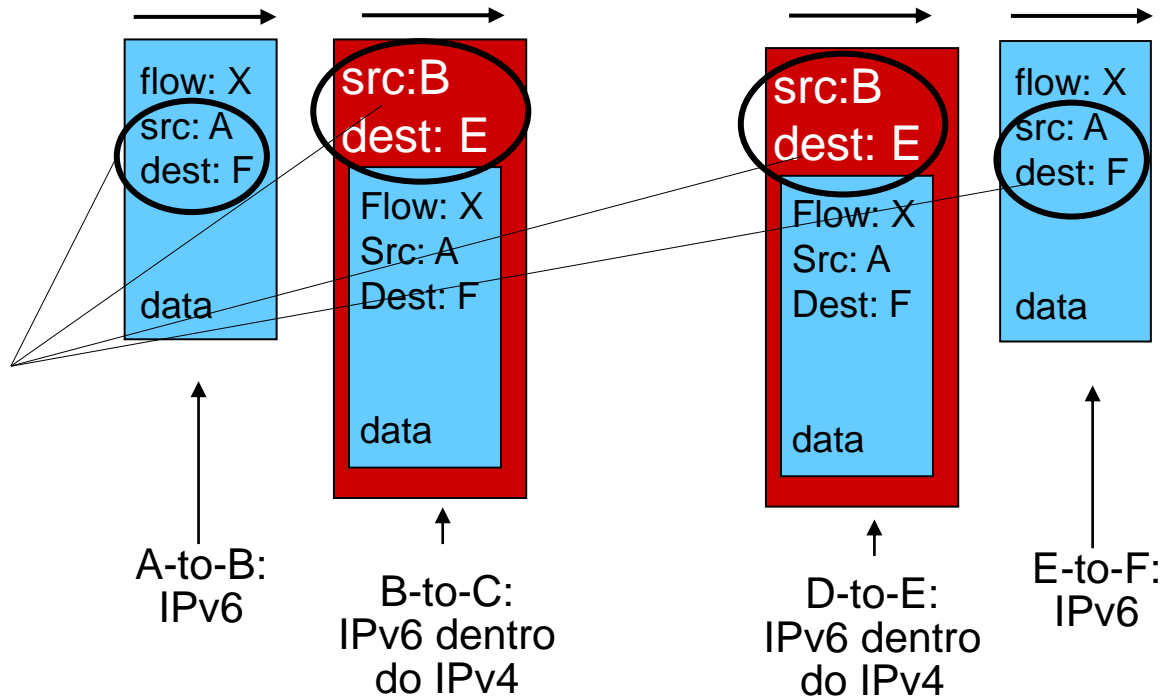
Visão lógica:



Visão física:



Repare nos  
endereços  
fonte e destino!



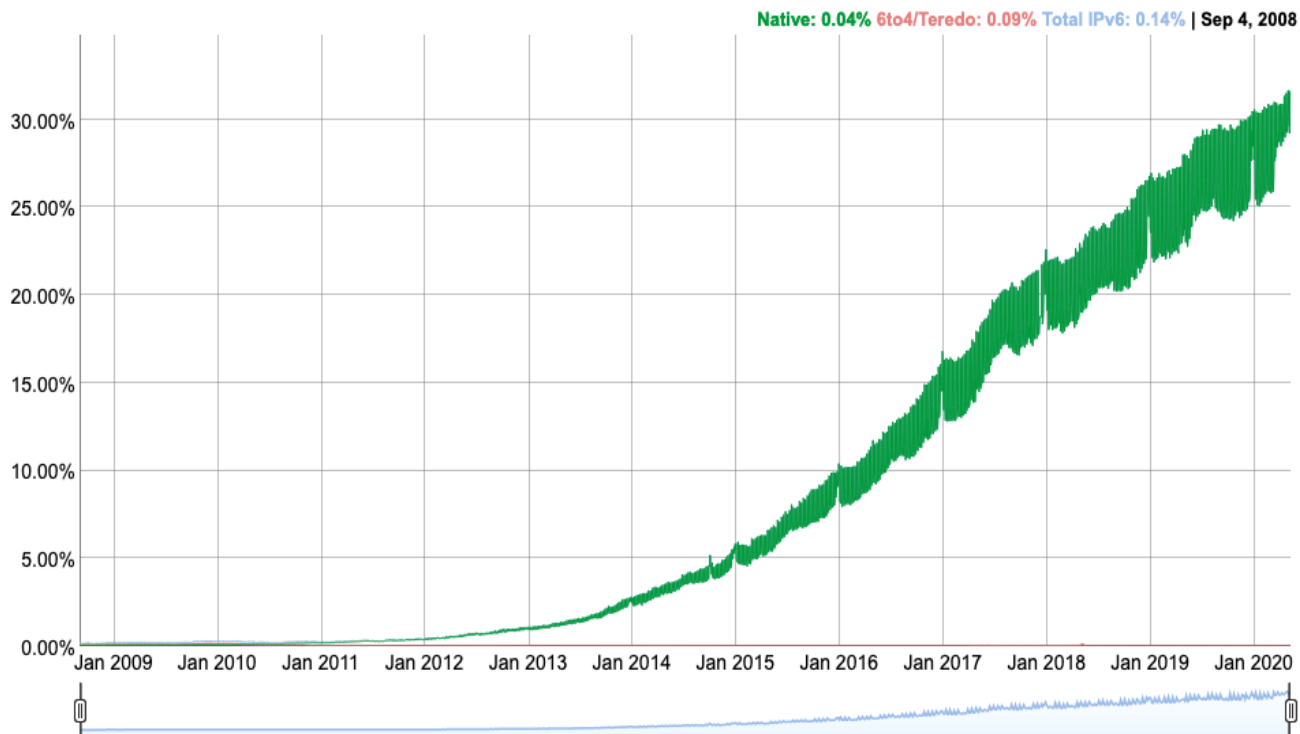
# IPv6: adoção

**Google:** ~30% dos clientes acessam serviços via IPv6

**NIST:** 1/3 de todos domínios do governo dos USA estão aptos a trabalharem 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.



1

<https://www.google.com/intl/en/ipv6/statistics.html>

# IPv6: adoção

*Google*: ~30% dos clientes acessam serviços via IPv6

NIST: 1/3 de todos domínios do governo dos USA estão aptos a trabalharem com IPv6

*Longo tempo para desenvolvimento e uso*

25 anos e continuando!

Pensem nas mudanças no nível de aplicação nos últimos 25 anos: www, mídia em redes sociais, video/audio streaming, jogos, videoconferência

*Por que?*

# ICMP: Internet Control Message Protocol

- ❑ Usado por computadores e roteadores para troca de informação de controle da camada de rede
  - ✓ relatório de erros: host, rede, porta ou protocolo inalcançáveis
  - ✓ echo request/reply (usado pela aplicação ping)
- ❑ Como se fosse uma camada "acima" do IP:
  - ✓ mensagens ICMP são transportadas em datagramas IP
- ❑ **Mensagem ICMP:** tipo, código, mais os primeiros 8 bytes do datagrama IP que causou o erro

# Protocolo de Mensagens de Controle da Internet (ICMP)

## Tipos de mensagens ICMP

Tipo ICMP	Código	Descrição
0	0	resposta de eco (para <i>ping</i> )
3	0	rede de destino inalcançável
3	1	hospedeiro de destino inalcançável
3	2	protocolo de destino inalcançável
3	3	porta de destino inalcançável
3	6	rede de destino desconhecida
3	7	hospedeiro de destino desconhecido
4	0	repressão da origem (controle de congestionamento)
8	0	solicitação de eco
9	0	anúncio do roteador
10	0	descoberta do roteador
11	0	TTL expirado
12	0	cabeçalho IP inválido

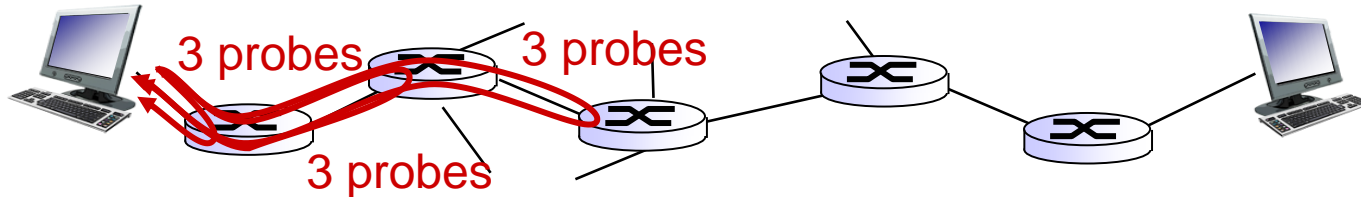
# ICMP - Ex.: traceroute (Linux)

- ❑ Origem envia uma série de segmentos UDP em direção ao destino
  - ✓ com TTLs crescentes: 1, 2, 3, ...
- ❑ Ao receber o n-ésimo datagrama, o n-ésimo roteador observa que seu TTL zerou
  - ✓ envia de volta mensagem ICMP tipo 11, código 0, com nome e endereço IP do enésimo roteador
- ❑ Host de origem recebe cada uma das mensagens ICMP e:
  - ✓ reconstitui a rota para o host destino
  - ✓ De acordo com o valor do RTT, estima o atraso acumulado em cada nó no caminho
  - ✓ no Windows: ver *tracert*

# Traceroute e ICMP

## *Critério de parada:*

- ❖ Segmento UDP chega no destino com um n° de porta não utilizado
- ❖ Destino retorna a mensagem ICMP “porta inalcançável” (tipo 3, código 3)  $\Rightarrow$  origem para de enviar pacotes



# Tornando o roteamento escalável

## Problemas do mundo real

- ❑ roteadores não são todos idênticos
- ❑ na prática, a Internet é heterogênea: as redes possuem diferentes topologias e algoritmos de roteamento

### Escala: bilhões de destinos

- ❑ Não é possível armazenar todos os destinos numa única tabela de rotas!
- ❑ As mudanças na tabela de rotas irão congestionar os enlaces!

### Autonomia Administrativa

- ❑ Internet = rede de redes
- ❑ Cada administração de rede pode querer controlar o roteamento na sua própria rede



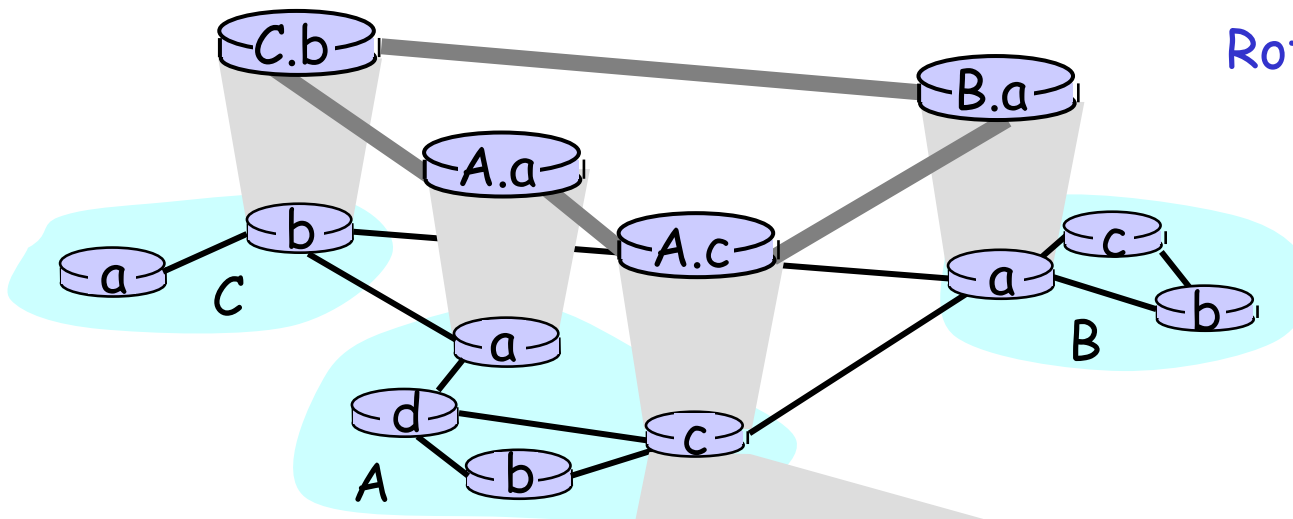
# Abordagem da Internet p/ roteamento escalável

- ❑ Agrega roteadores em regiões: "sistemas autônomos" (AS)
- ❑ Roteadores no mesmo AS rodam o mesmo protocolo de roteamento
  - ✓ Protocolo de roteamento "Intra-AS"
- ❑ Roteadores em diferentes AS's podem rodar diferentes protocolos de roteamento

## roteadores de borda

- ❑ Roteadores de interface de um AS com outros AS's
  - ❑ Rodam protocolos de roteamento intra-AS com os outros roteadores do mesmo AS
  - ❑ Também são responsáveis por enviar mensagens para fora do AS
- ↓
- ❑ Rodam *protocolo de roteamento inter-AS* com outros roteadores de borda (de outros AS's)

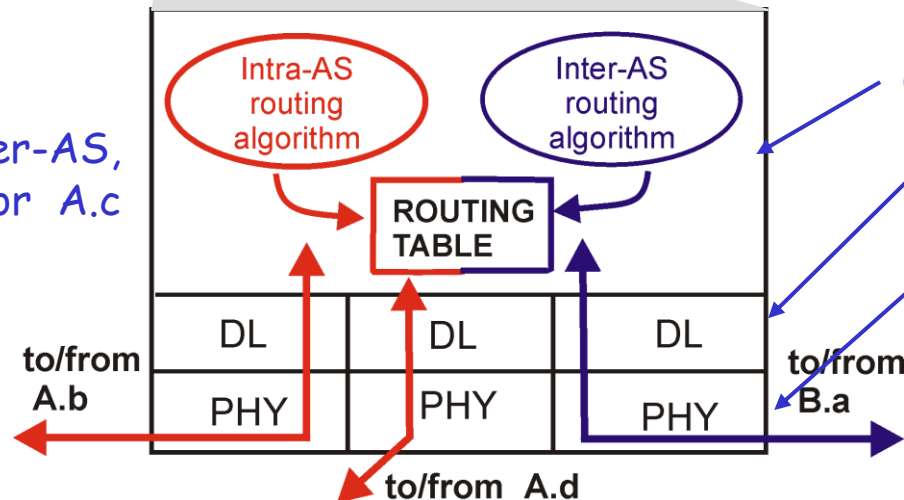
# Roteamento Intra-AS e Inter-AS



## Roteadores de Borda

- realizam roteamento **inter-AS** entre si
- realizam roteamento **intra-AS** com outros roteadores do mesmo AS

Roteamento inter-AS,  
intra-AS no roteador A.c



Camada de rede

Camada de enlace

Camada física

# AS's interconectadas

Tabela de roteamento é configurada por ambos algoritmos,  
intra-AS e inter-AS

Intra-AS estabelece entradas para destinos internos

Inter-AS e intra-As estabelecem entradas para destinos  
externos

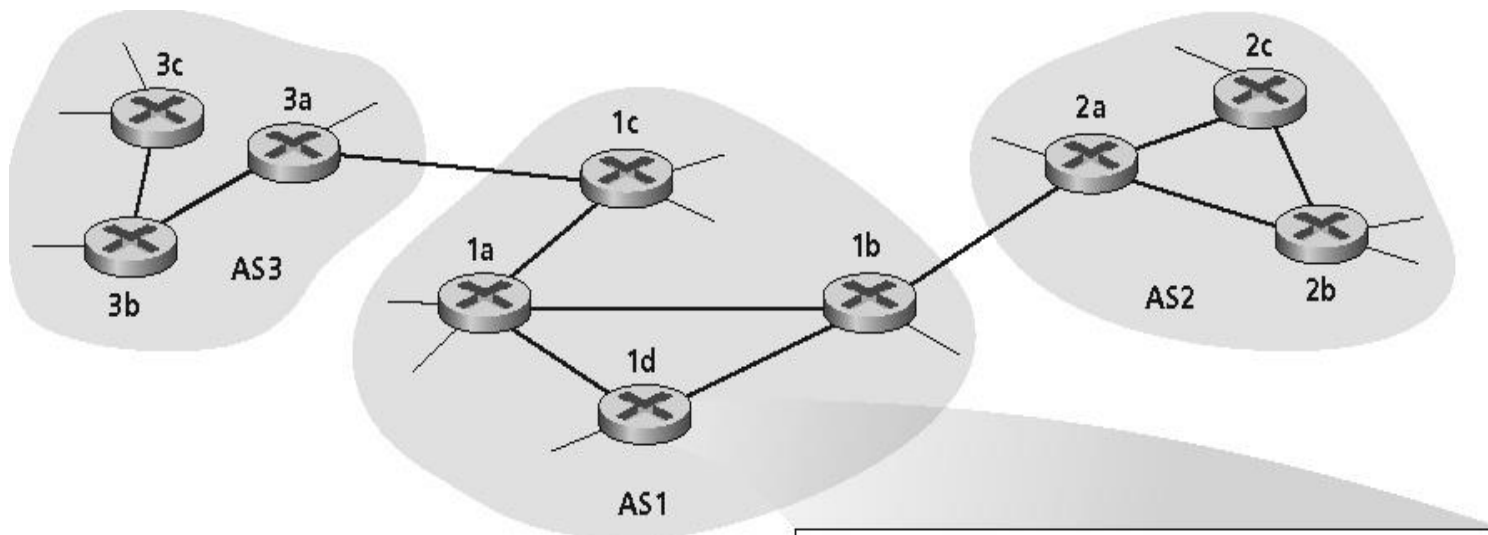
# Tarefas Inter-AS

Q: Suponha que um roteador no AS1 receba um datagrama cujo destino seja fora do AS1. O roteador deveria encaminhar o pacote para os roteadores de borda, mas qual deles?

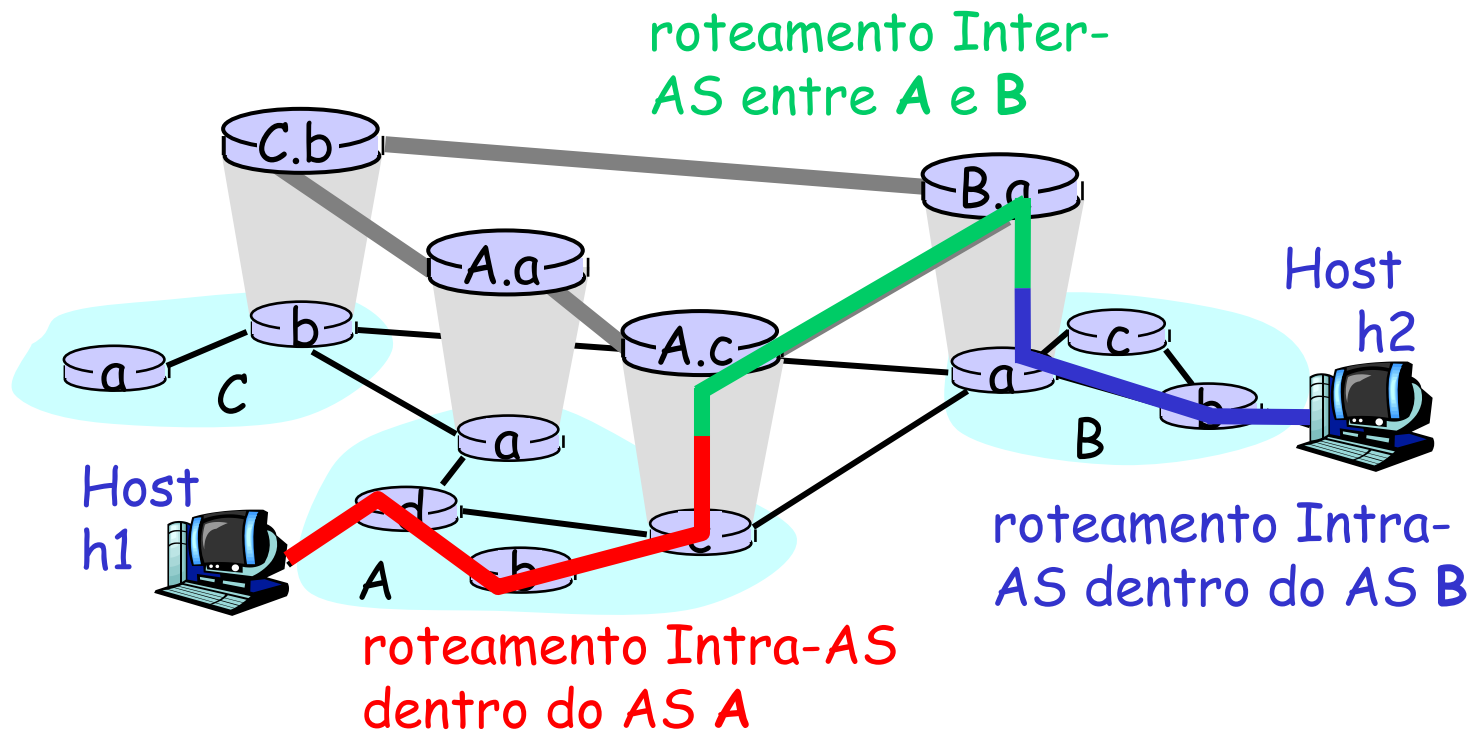
**Roteador de borda em AS1 precisa:**

1. Aprender quais destinos são alcançáveis através de AS2 e através de AS3.
2. Propagar suas informações de alcance para todos os roteadores em AS1.

**Tarefa para o protocolo de roteamento inter-AS!**



# Roteamento Intra-AS e Inter-AS



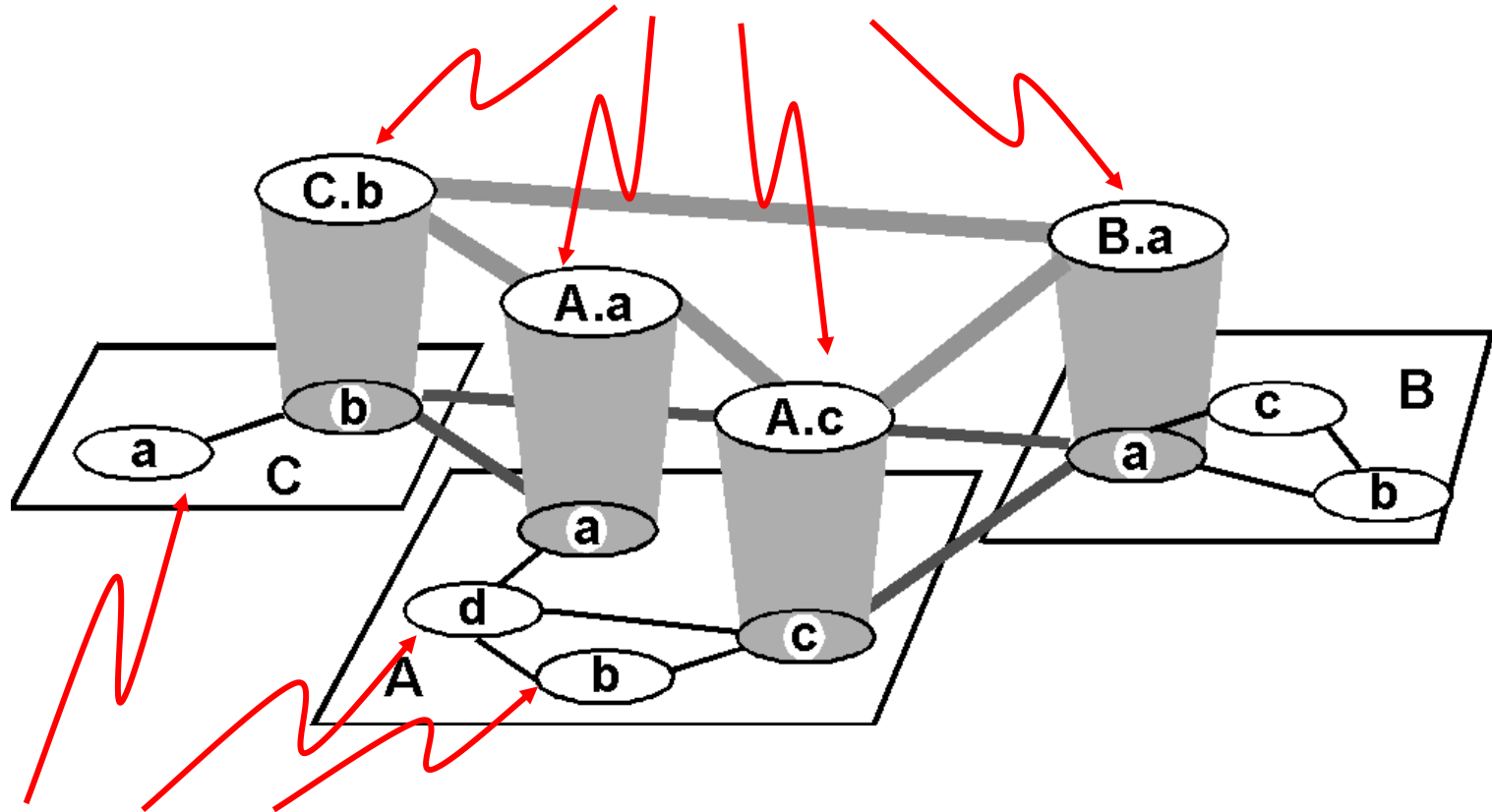
- Rotas fim-a-fim (h1 p/ h2) são obtidas por meio da concatenação de rotas internas em vários AS's e através das rotas inter-AS.

# Roteamento na Internet

- ❑ A Internet consiste de **Sistemas Autônomos (AS)** interconectados entre si:
  
- ❑ Dois níveis de roteamento:
  - ✓ **Intra-AS:** o administrador é responsável pela definição do método de roteamento
  
  - ✓ **Inter-AS:** padrão único

# Hierarquia de AS

Roteador de borda Inter-AS



Roteador interno Intra-AS

# Roteamento Intra-AS

Protocolos de roteamento intra-AS mais comuns:

- ✓ RIP: Routing Information Protocol (RFC 1723)
  - ✓ DV clássico: DVs trocados a cada 30 segundos
  - ✓ Atualmente não é muito usado
- ✓ EIGRP: Enhanced Interior Gateway Routing Protocol (proprietário da Cisco até 2013)
  - ✓ Baseado em DV
- ✓ OSPF: Open Shortest Path First (RFC 2328)
  - ✓ Roteamento baseado no estado de enlace



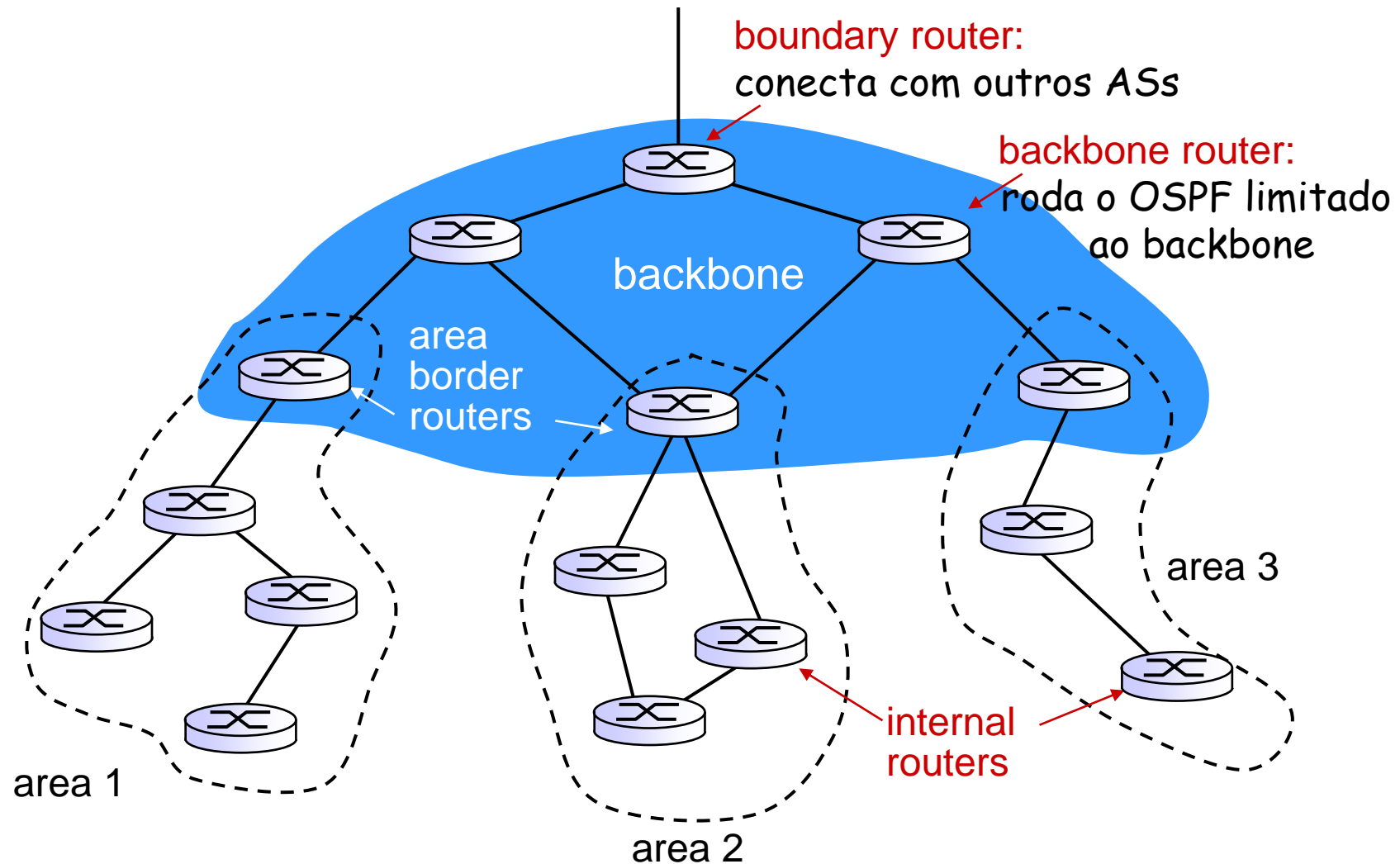
# OSPF (Open Shortest Path First)

- ❑ Significado de "open": publicamente disponível
- ❑ Usa algoritmo do tipo *Link State*
  - ✓ disseminação de pacotes de anúncio LS
  - ✓ Possíveis métricas de custo dos enlaces: banda e atraso
  - ✓ mapa topológico em cada nó
  - ✓ usa algoritmo de Dijkstra para cálculo de rotas
- ❑ Anúncios são distribuídos para todo o AS (via "inundação")
  - Mensagens transmitidas diretamente sobre IP (ao invés de sobre TCP ou UDP)

## OSPF características avançadas (RIP não possui)

- ❑ **Segurança:** todas as mensagens OSPF são autenticadas (para prevenir intrusão de hackers)
- ❑ **Múltiplos caminhos** de mesmo custo são permitidos (o RIP só permite um caminho para cada destino)
- ❑ Podem ser usadas **múltiplas métricas** para diferentes tipos de serviços (TOS) (ex.: custo de enlace por satélite definido como baixo para tráfego de "melhor esforço" e alto para serviços de tempo real)

# OSPF Hierárquico



# OSPF Hierárquico

Hierarquia de dois níveis: área local e backbone.

- anúncios de Link-state são enviados apenas nas áreas locais ou backbone
- cada nó tem a topologia detalhada da área, mas somente direções conhecidas (caminhos mais curtos) para redes em outra áreas.

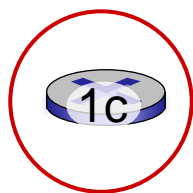
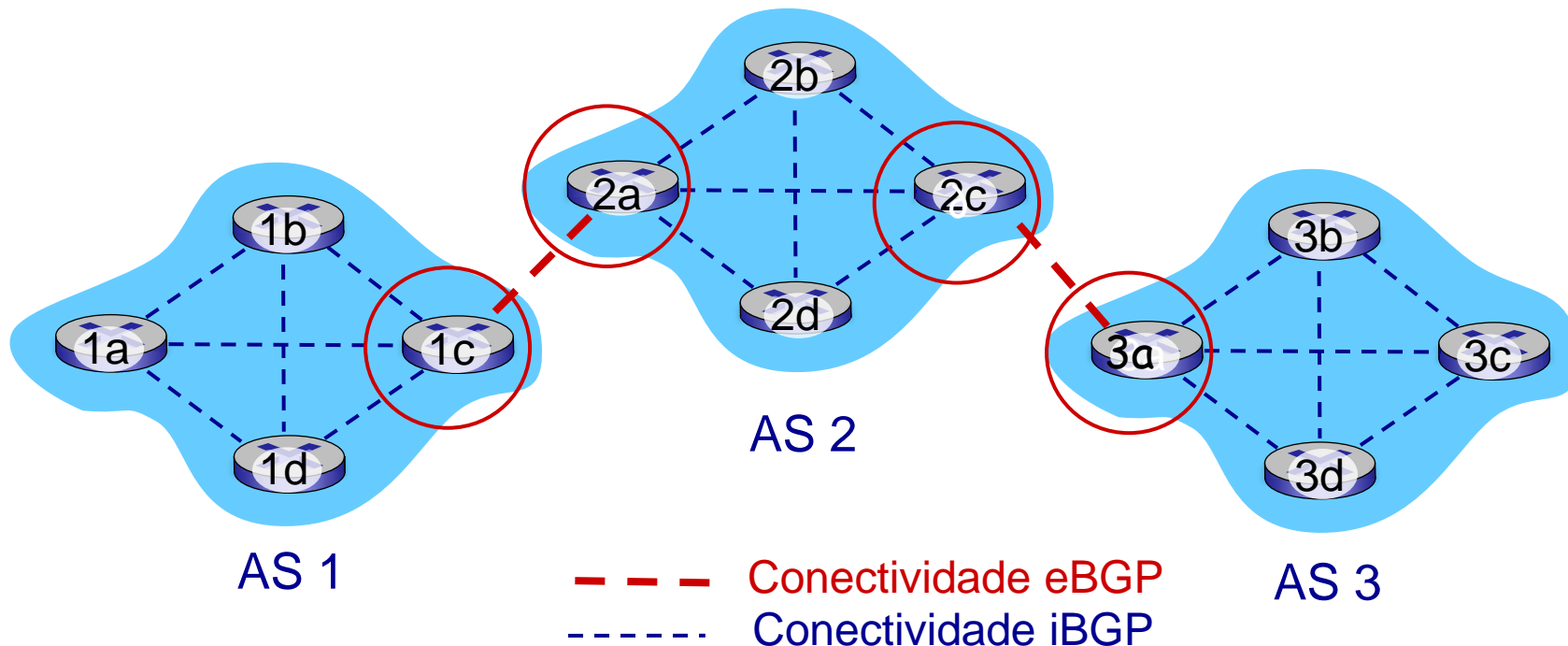
# OSPF Hierárquico

- ❑ **Roteadores locais:**
  - difunde os anúncios LS somente na área
  - cálculo de roteamento dentro da área
  - encaminha pacotes para fora da área via roteador de borda de área
- ❑ **Roteadores de borda de área:** “resumem” distâncias para destinos na própria área e enviam para outros roteadores de borda de área
- ❑ **Roteadores de backbone:** executam o roteamento OSPF de forma limitada ao backbone.
- ❑ **Roteadores de borda do AS:** realizam as funções de interconexão com outros sistemas autônomos

# Roteamento inter-AS na Internet: BGP

- ❖ **BGP (Border Gateway Protocol):** protocolo de roteamento interdomínio "de fato"
  - "cola" que une a Internet
- ❖ BGP provê a cada AS meios de:
  - **eBGP: conexão BGP externa** - obtém informações de alcançabilidade de uma sub-rede a partir dos ASs vizinhos.
  - **iBGP: conexão BGP interna** - propaga informações de alcançabilidade para todos os roteadores internos do AS.
  - Determina "boas" rotas para outras sub-redes baseado em informações de alcançabilidade e de política.
- ❖ Permite a uma sub-rede anunciar sua existência para o resto da Internet (e os destinos que ela pode alcançar): *"Estou aqui!"*

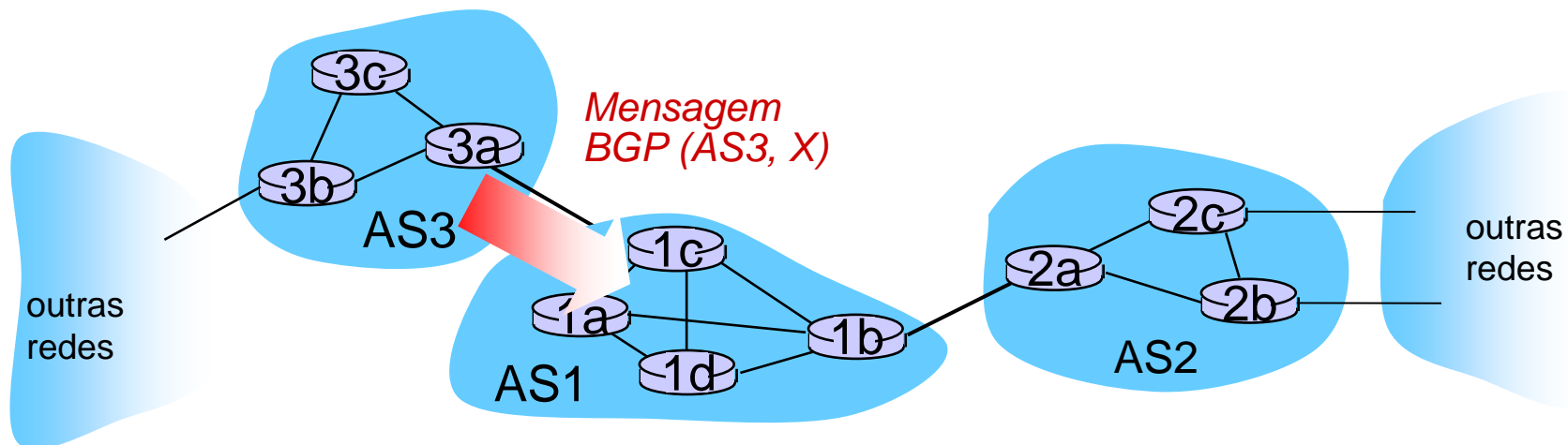
# Conexões eBGP e iBGP



Roteadores de *borda* rodam ambos os protocolos (eBGP e iBGP)

# BGP: básico

- ❖ Sessão BGP: 2 roteadores BGP (“pares”) trocam mensagens BGP:
  - anunciando *caminhos* para diferentes destinos (prefixos de redes) (BGP é um protocolo “path vector”)
  - trocadas sobre conexões TCP que usam a porta 179
- ❖ qdo AS3 (rot. 3a) anuncia um prefixo (AS3, X) para AS1 (rot. 1c)  
AS3 *promete* a AS1 que repassará datagramas para X  
AS3 pode agregar prefixos em seu anúncio

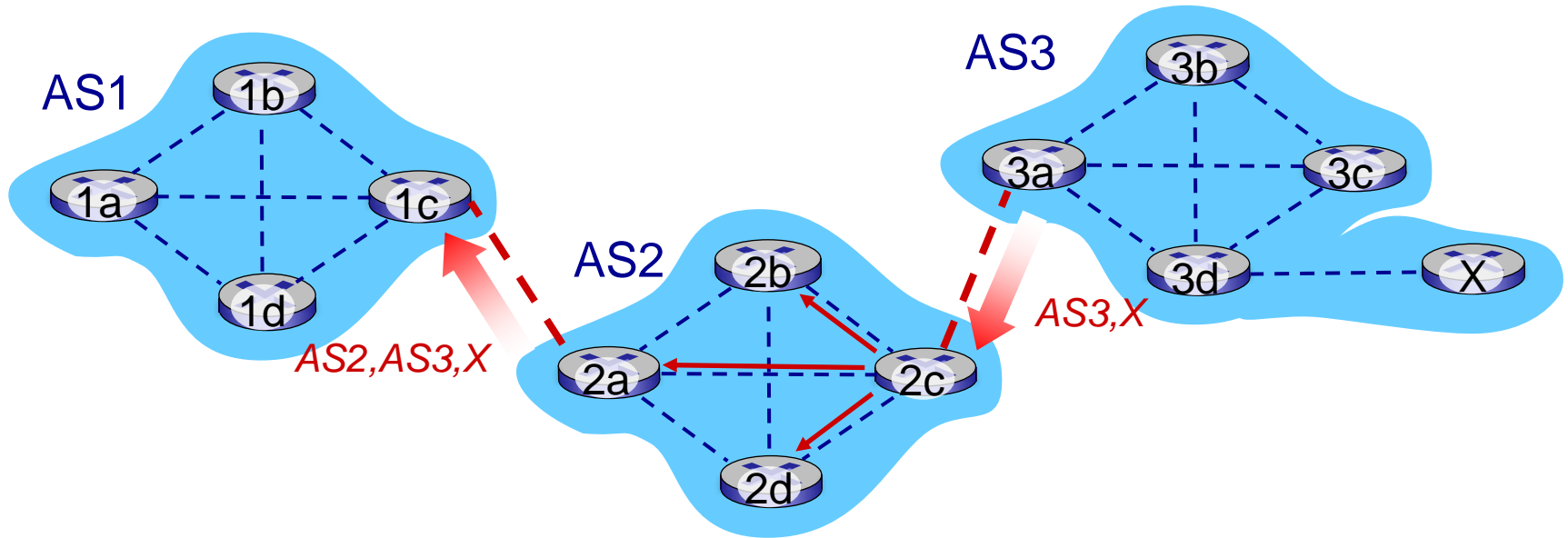




# Atributos de caminho e rotas BGP

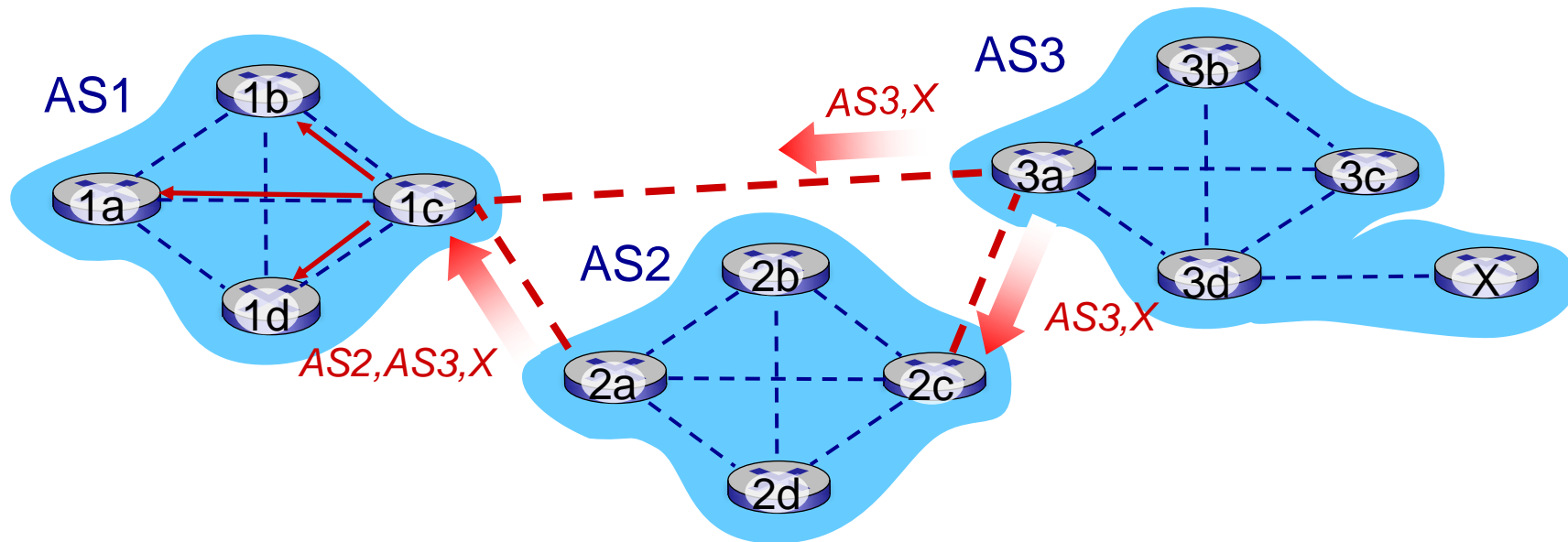
- ❑ Prefixo anunciado inclui vários atributos BGP  
prefixo + atributos = "rota"
- ❑ 2 importantes atributos:
  - **AS-PATH**: contém os ASs através dos quais os anúncios de prefixo foram passados. Por exemplo: AS67, AS17
  - **NEXT-HOP**: indica o roteador interno específico, dentro do AS atual, que será usado para atingir o próximo AS
- ❑ **Roteamento baseado em Política**:
  - roteador de borda recebendo o anúncio de rota usa **política** para aceitar/rejeitar um anúncio de caminho  
ex.: nunca rotear através do AS X ("**policy-based** routing")
  - a política do AS também determina se deve ou não ser anunciado o caminho para outros ASs vizinhos

# Anúncios de caminhos (BGP path)



- roteador 2c, de AS2, recebe o anúncio de caminho **AS3,X** (via eBGP) do roteador 3a, de AS3
  - ✓ Baseado na política de AS2, roteador 2c aceita o caminho AS3,X e o propaga (via sessão iBGP) para todos os roteadores de AS2
  - ✓ Baseado na política de AS2, roteador 2a anuncia (via eBGP) o caminho **AS2, AS3, X** para o roteador 1c, de AS1

# Anúncios de caminhos (BGP path)



Um roteador de borda pode aprender **múltiplos** caminhos para o destino. Ex:

○ roteador 1c, de AS1, aprende o caminho **AS2,AS3, X** via anúncio feito por 2a, mas também....

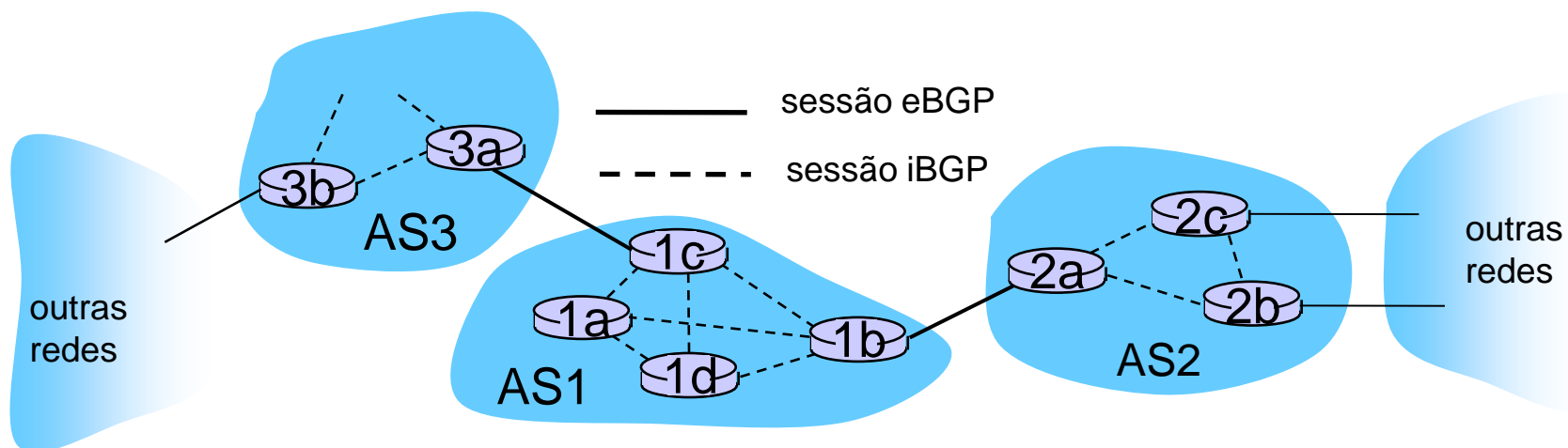
- Aprende o caminho **AS3, X** via 3a
- Baseado na política de AS1, o roteador 1c escolhe o caminho **AS3, X** e o **anuncia dentro de AS1 via iBGP**

# Mensagens BGP

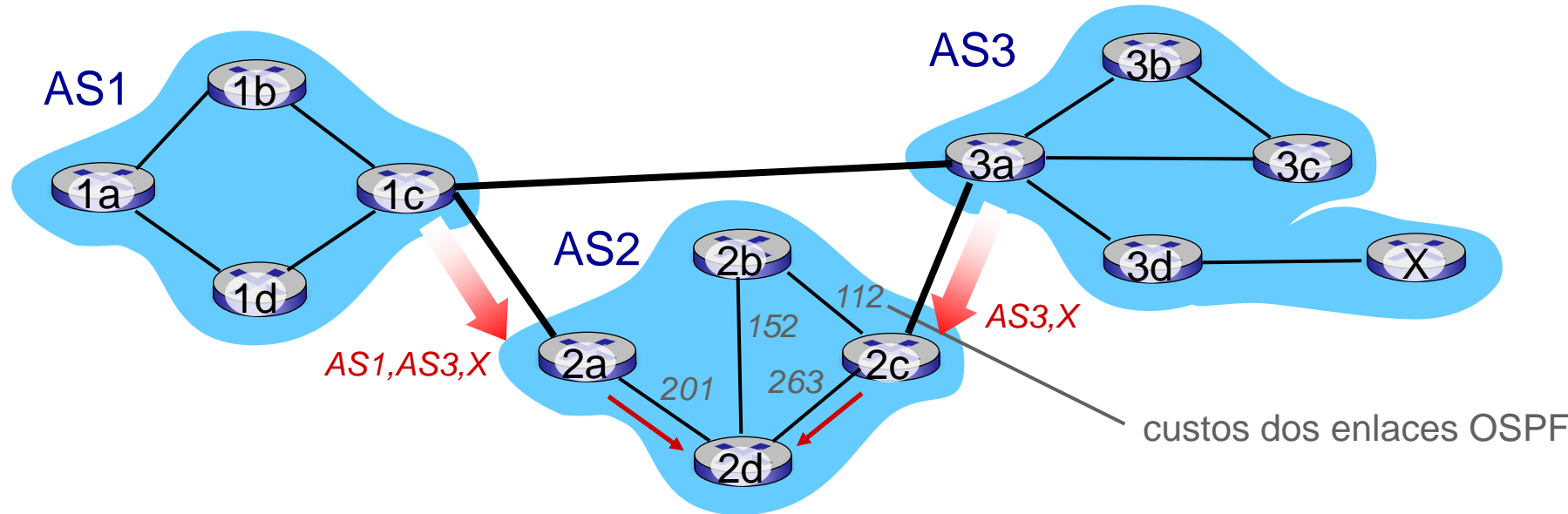
- ❑ As mensagens do BGP são trocadas entre pares sobre conexões TCP.
- ❑ mensagens BGP:
  - ✓ **OPEN**: inicia a conexão TCP com um roteador parceiro e autentica o transmissor BGP
  - ✓ **UPDATE**: anuncia novo caminho (ou retira uma rota antiga, que não é mais válida)
  - ✓ **KEEPALIVE** mantém a conexão viva em caso de ausência de atualizações; também reconhece (ACK) mensagens de requisição OPEN
  - ✓ **NOTIFICATION**: reporta erros nas mensagens anteriores; também usado para encerrar uma conexão

# BGP: anúncio de caminho

- usando sessão eBGP entre 3a e 1c, AS3 envia prefixos com info de alcançabilidade para AS1.
  - 1c pode usar iBGP p/ distribuir novas info de prefixos dentro de AS1
  - 1b pode "re-anunciar" novas info de alcançabilidade p/ AS2 sobre uma sessão eBGP em 1b-2a
- qdo o roteador aprende sobre novos prefixos, ele cria entradas para estes em sua tabela de repasse.



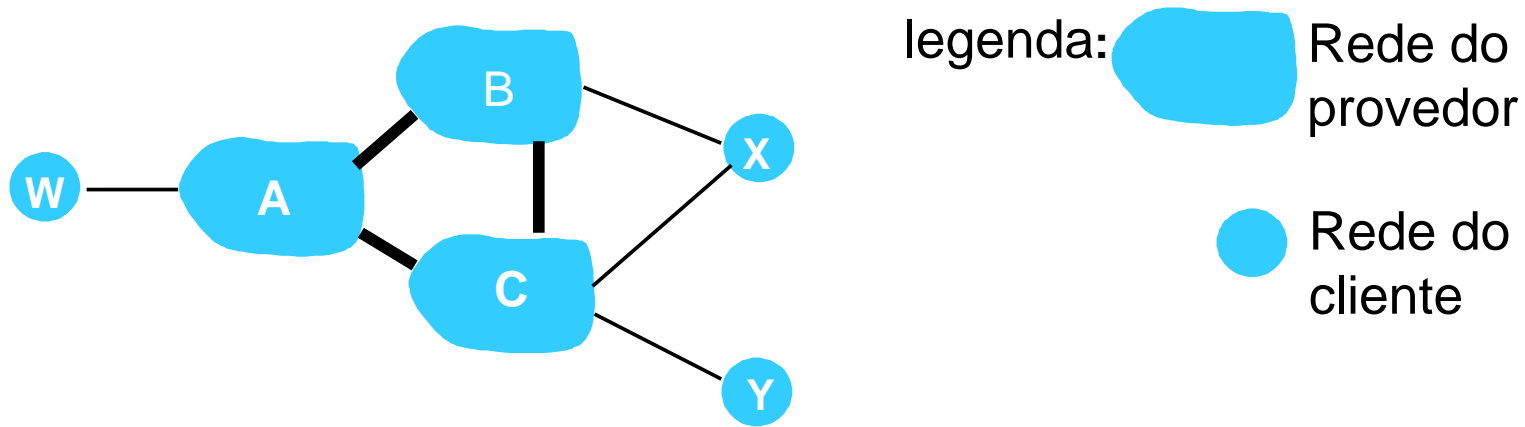
# Roteamento de "Batata Quente"



2d aprende (via iBGP) que pode rotear p/ X via 2a ou 2c

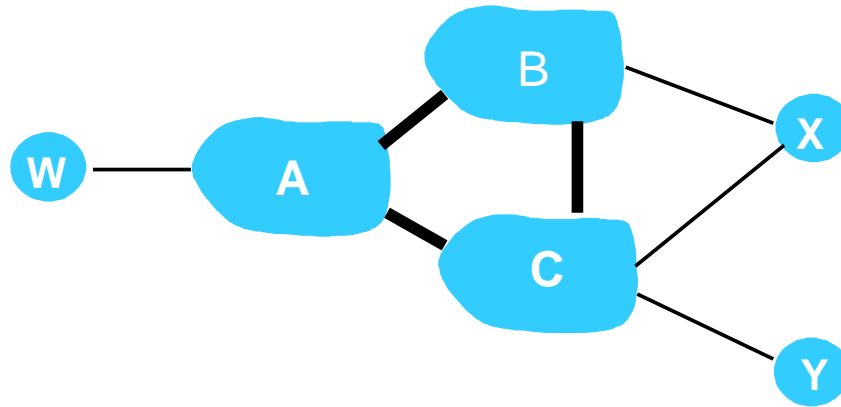
**Roteamento batata quente:** escolhe o roteador local que tem o menor custo intra-domínio (ex., 2d escolhe 2a, apesar de passar por mais AS's p/ X): não se preocupa com o custo inter-domínio!

# BGP: atingindo a política via anúncios (1)



- ❖ A,B,C são *redes provedoras*
- ❖ X,W,Y são clientes (destes provedores)
- ❖ X é *interligada a 2 provedores*
  - X não quer rotear tráfego de B para C
  - .. então X não anuncia para B a rota para C

# BGP: atingindo a política via anúncios (2)



- ❖ A anuncia o caminho A,W para B
- ❖ B anuncia o caminho B,A,W para X
- ❖ B deve anunciar o caminho B,A,W para C?
  - Não! Porque nem W e nem C são clientes de B
  - B quer forçar C a rotear para w via A
  - B quer rotear *somente para seus clientes!*



# Critérios de seleção de rota BGP

Roteador pode aprender mais de uma rota p/ o AS de destino. Seleciona rota baseado, por exemplo, em:

1. Valor de preferência local: decisão política
2. Menor AS-PATH
3. Roteador de NEXT-HOP mais próximo: roteamento de "batata quente"

# Porque os protocolos Intra-AS e Inter-AS são diferentes?

## Política:

- ❑ Inter-AS: a administração quer ter controle sobre como seu tráfego é roteado e sobre quem roteia através da sua rede.
- ❑ Intra-AS: administração única: não há necessidade de decisões políticas

## Escalabilidade:

- ❑ O roteamento hierárquico poupa espaço da tabela de rotas e reduz o tráfego de atualização

## Desempenho:

- ❑ Intra-AS: preocupação maior é desempenho
- ❑ Inter-AS: regras de mercado (políticas) podem ser mais importantes que desempenho