

CAP 6. CAMADA DE REDE

AULA 1: INTRODUÇÃO E ENDEREÇOS IP

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://MOODLE.UFSC.BR)

Capítulo 2

Camada de aplicação

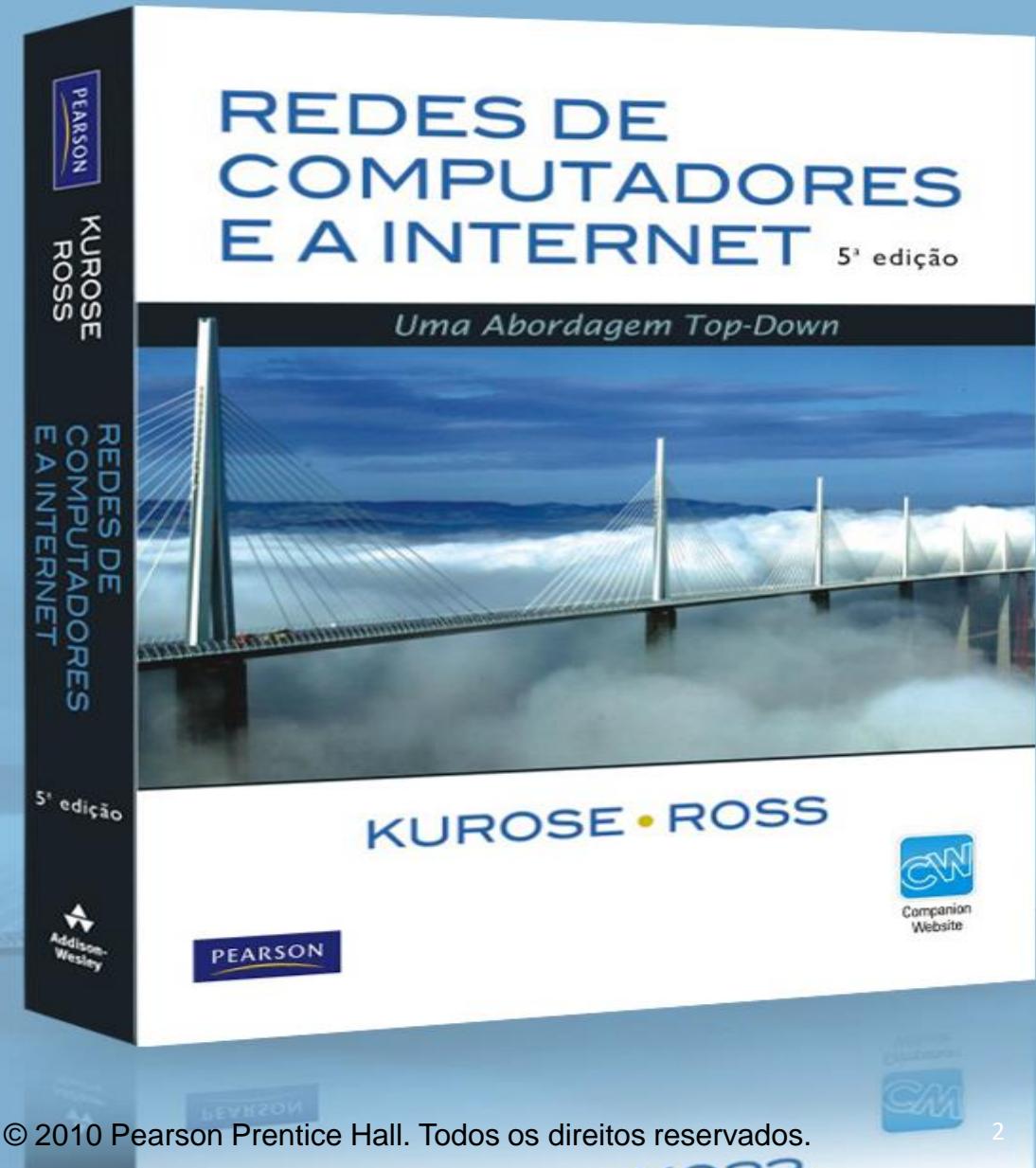
Nota sobre o uso destes slides ppt:

Estamos disponibilizando estes slides gratuitamente a todos (professores, alunos, leitores). Eles estão em formato do PowerPoint para que você possa incluir, modificar e excluir slides (incluindo este) e o conteúdo do slide, de acordo com suas necessidades. Eles obviamente representam *muito* trabalho da nossa parte. Em retorno pelo uso, pedimos apenas o seguinte:

- Se você usar estes slides (por exemplo, em sala de aula) sem muita alteração, que mencione sua fonte (afinal, gostamos que as pessoas usem nosso livro!).
- Se você postar quaisquer slides sem muita alteração em um site Web, que informe que eles foram adaptados dos (ou talvez idênticos aos) nossos slides, e inclua nossa nota de direito autoral desse material.

Obrigado e divirta-se! JFK/KWR

Todo o material copyright 1996-2009
J. F Kurose e K. W. Ross, Todos os direitos reservados.



Pilha de protocolos Internet

Aplicação: dá suporte às aplicações de rede

- HTTP, FTP, SMTP, ...

Transporte: transferência de dados host-a-host
(processo-a-processo)

- TCP, UDP

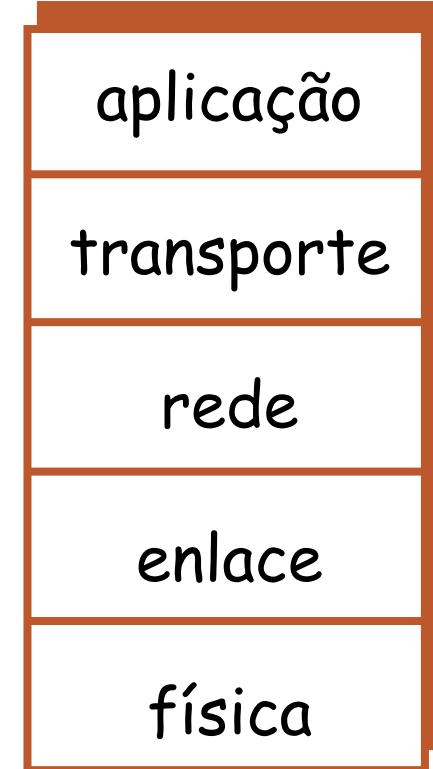
Rede: roteamento de datagramas da origem até o destino

- IP, protocolos de roteamento

Enlace: transferência de dados entre elementos de rede vizinhos

- Ethernet

Física: bits “no fio”



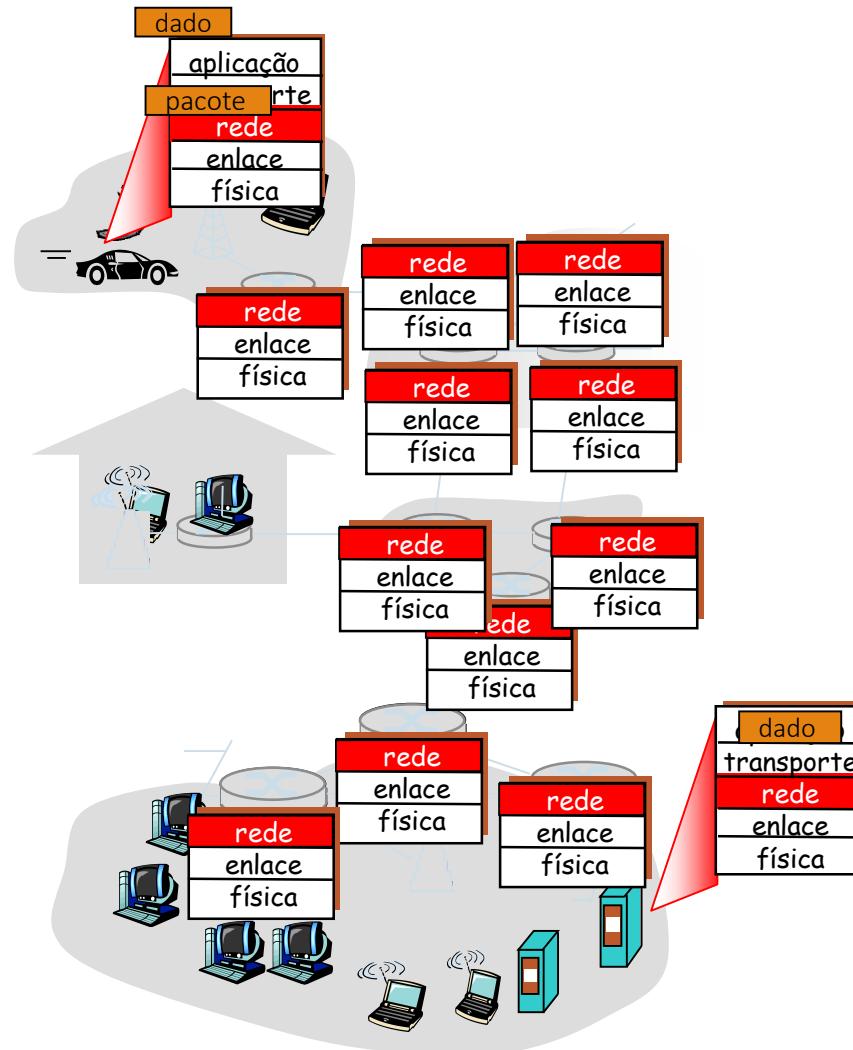
Cap 6. Camada de rede

Plano do capítulo

- Introdução: funções básicas da camada de rede
- Camada de rede da Internet
- Endereçamento IP
- Mapeamento de endereços: ARP e RARP
- Atribuindo endereços IP
- NAT
- Formato do datagrama IP
- Fragmentação e remontagem de datagramas IP
- ICMP Internet Control Message Protocol
- Protocolos de roteamento
- Arquitetura do Roteador
- IPv6

Introdução: Camada de rede

- Encaminha segmentos de transporte do hosp. emissor ao receptor
- Camada distribuída: no emissor, receptor e nós intermediários
- Lado emissor encapsula segmentos em datagramas
- Roteador examina campos de cabeçalho em todos os datagramas IP que passam por ele



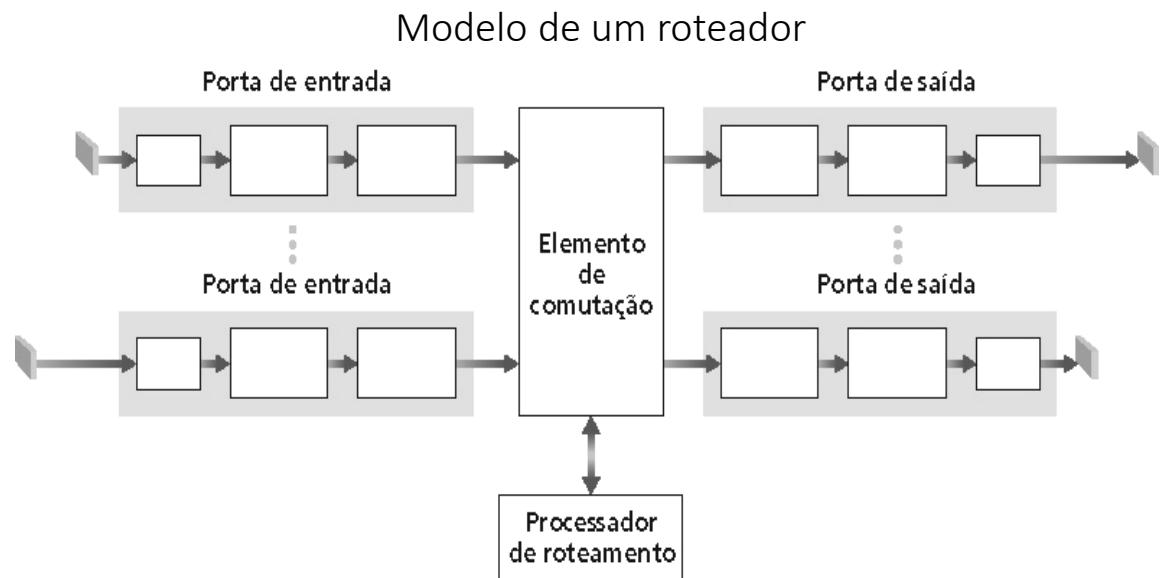
Duas importantes funções da camada de rede

Repassar (Comutação)

- Mover pacotes da entrada do roteador para a saída apropriada do roteador
- Analogia: processo de passar por um único cruzamento

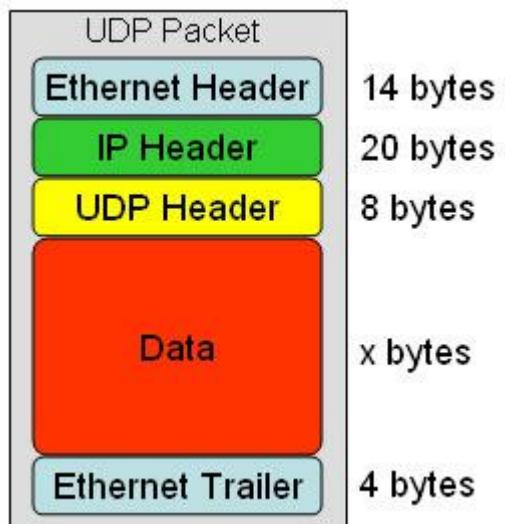
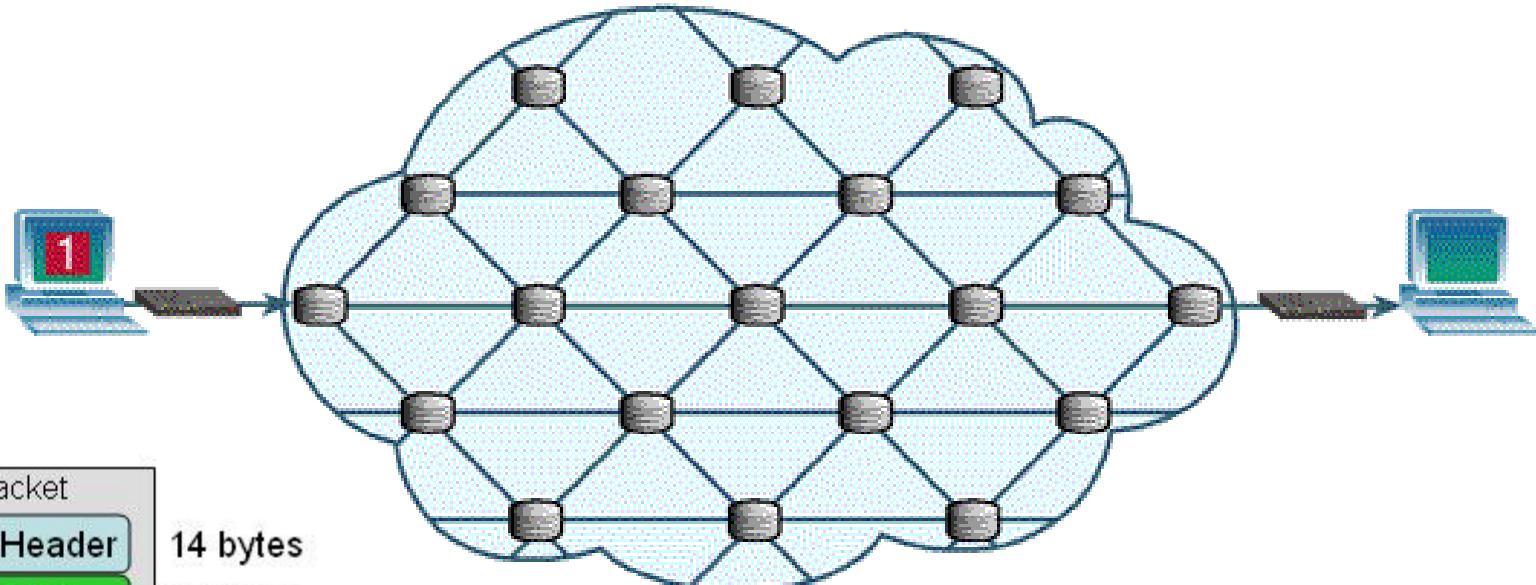
Roteamento

- Determinar rota seguida pelos pacotes da origem ao destino via algoritmos de roteamento
- Analogia: processo de planejar uma viagem da origem ao destino



Redes de datagrama

Roteamento de pacotes pela rede WAN/Internet



Introdução: Camada de Rede

Algoritmos de roteamento determinam valores em tabelas de rotas

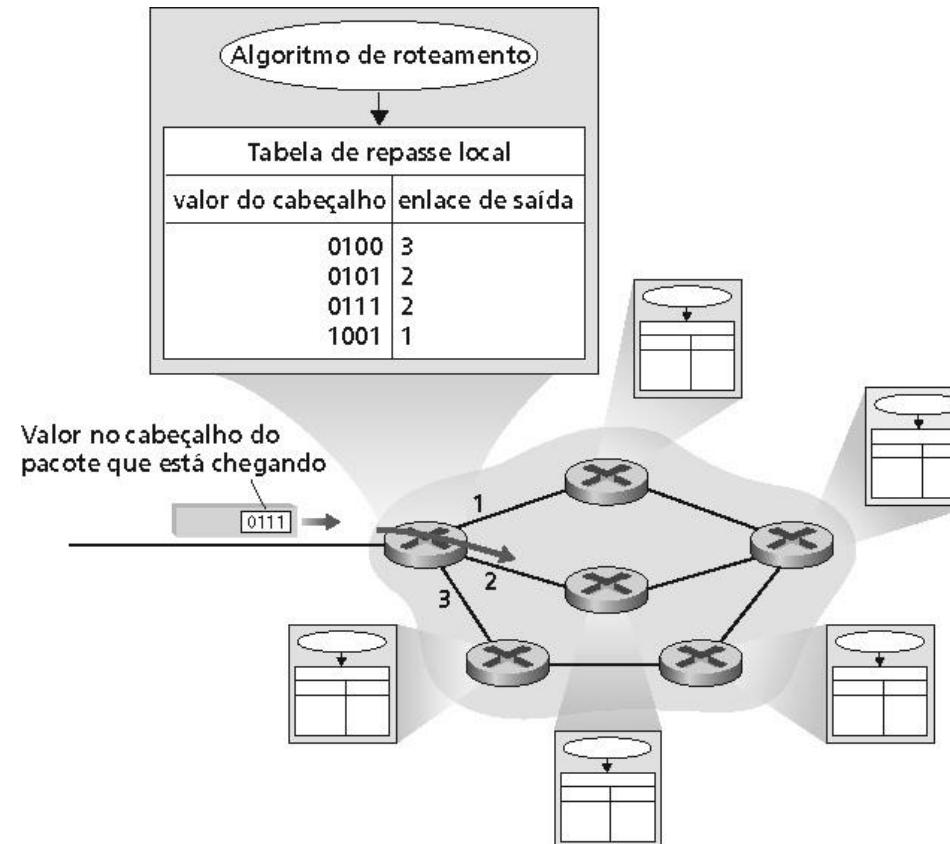


Tabela de comutação

4 bilhões de entradas possíveis

| Faixa de Endereços de Destino | Interface de Enlace |
|---|---------------------|
| 11001000 00010111 00010000 00000000 até 11001000 00010111 00010111 11111111 | 0 |
| 11001000 00010111 00011000 00000000 até 11001000 00010111 00011000 11111111 | 1 |
| 11001000 00010111 00011001 00000000 até 11001000 00010111 00011111 11111111 | 2 |
| senão | 3 |

Encontro de prefixos maiores

| Prefixo do endereço | Interface de Enlace |
|----------------------------|----------------------------|
| 11001000 00010111 00010 | 0 |
| 11001000 00010111 00011000 | 1 |
| 11001000 00010111 00011 | 2 |
| senão | 3 |

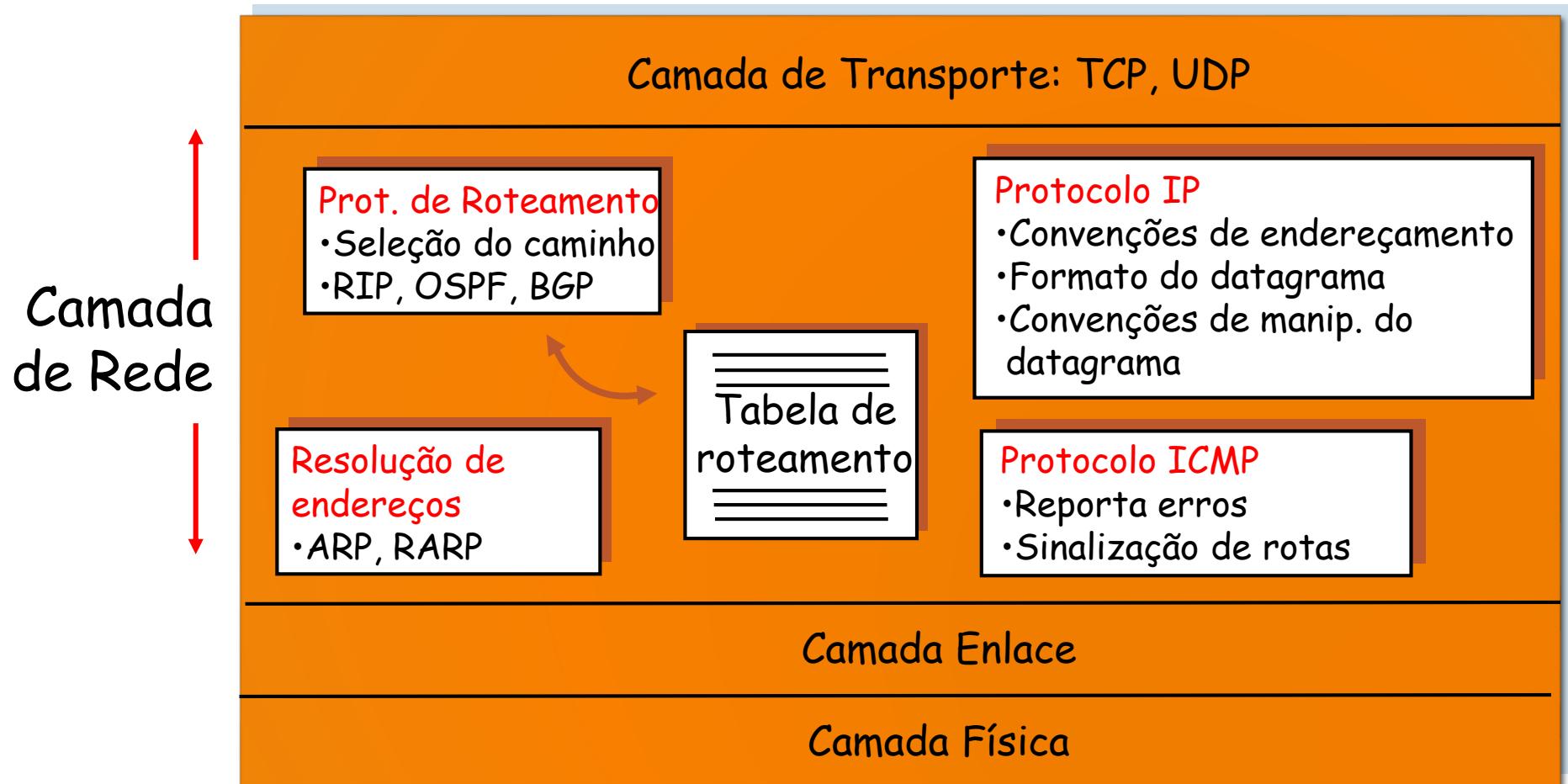
Exemplos

DA: 11001000 00010111 00010110 10100001 Qual interface?

DA: 11001000 00010111 00011000 10101010 Qual interface?

Camada de Rede da Internet

Funções da camada de rede de roteadores e hosts:



Tipos de Endereçamento

Endereçamento Horizontais

- O endereço não tem relação alguma com o lugar onde estão as entidades dentro da rede
 - Exemplo: endereços globalmente administrados (IEEE 802)
 - Constituído do número de assinatura do usuário
 - Exemplo: endereço MAC da placa de rede (camada de enlace)

Adaptador Ethernet Ethernet:

- Dificulta o roteamento
 - Não tem informações explícita sobre a localização da entidade
 - Facilita a mobilidade
 - Não necessita uma renumeração da entidade

Tipos de Endereçamento

Endereçamento Hierárquico

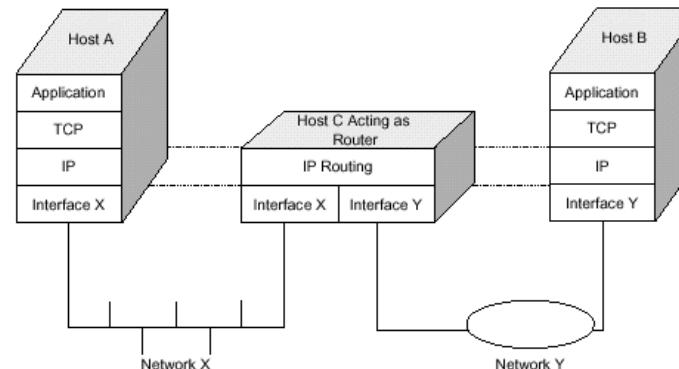
- O endereço de uma entidade é constituído de acordo com os endereços correspondentes aos vários níveis de hierarquia de que ela faz parte
- Exemplo: Redes Públicas de Pacote (recom. X.121)
 - Endereços são números decimais formados por três campos: código do país, código para a rede e um campo para endereçamento dentro da rede
- Exemplo: Endereço IP (Internet Protocol)
 - Identificação do host é formado pelo endereço da rede e pelo endereço do hospedeiro

```
Endereço IPv4. . . . . : 150.162.59.159(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.254.0
```

Endereçamento IP

Como Roteadores e Hosts são ligados a rede

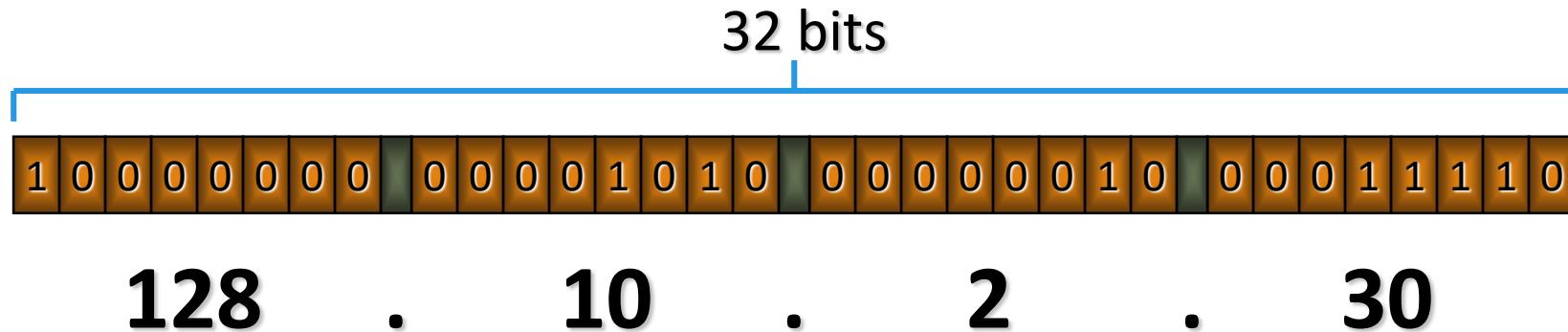
- Host típico tem apenas uma conexão para a rede (interface)
 - IP envia/recebe datagramas por esta interface
 - Tem um endereço IP
- Roteador tem geralmente diversas interfaces
 - Recebe datagramas de enlaces de entrada e envia para enlaces de saída
 - Tem vários endereços IP



Endereçamento IPv4

Notação Decimal Pontuada

- Exemplo:



Endereçamento IPv4

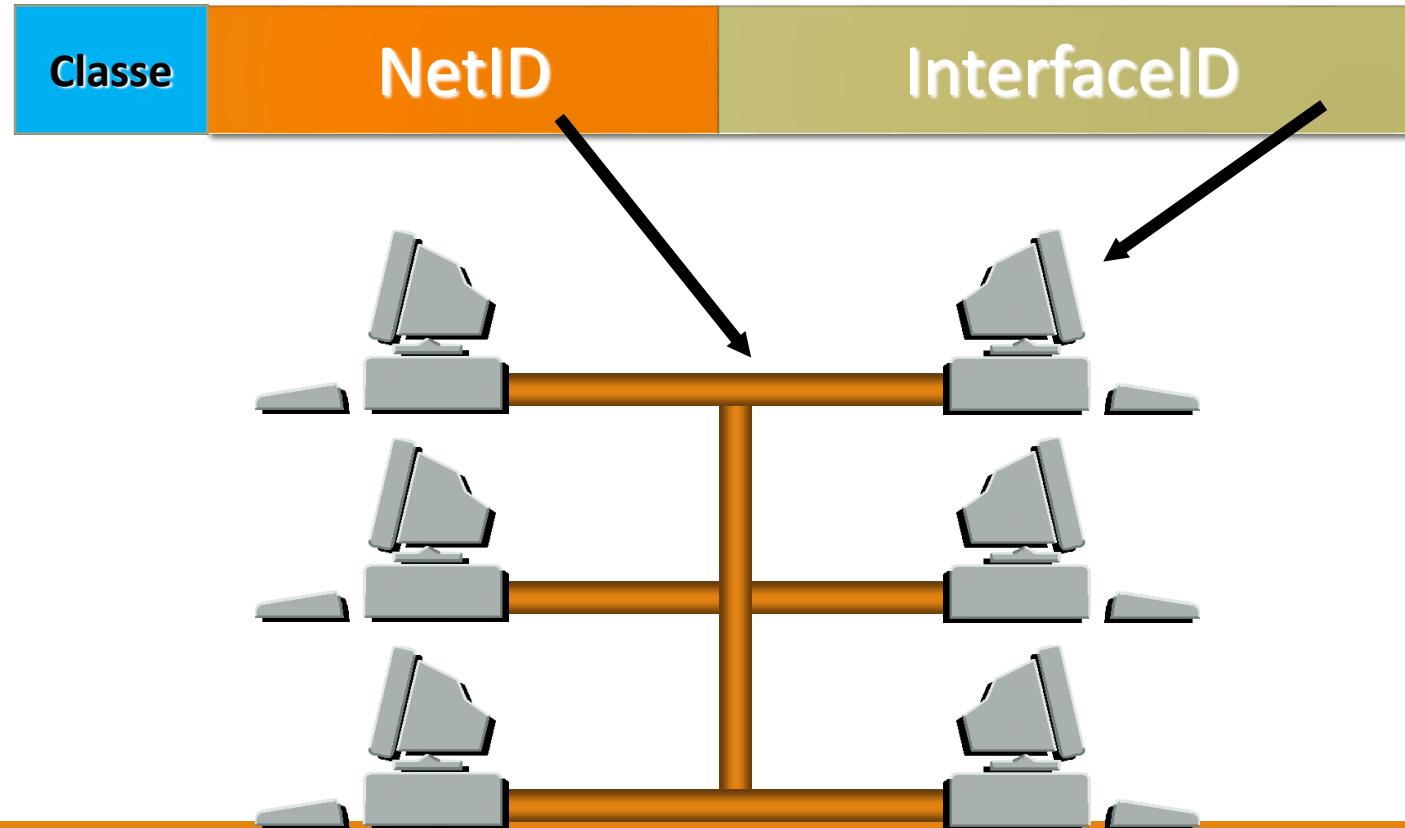
Capacidade de Endereçamento

- Palavra de 32 bits (4 bytes)
 - Por exemplo: 150.162.60.200
- Permite endereçar mais de 4 bilhões de máquinas
 - $2^{32} = 4.294.967.296$
 - Mas diversos endereços são reservados

Endereçamento IPv4

Endereçamento “class-full”:

- Redes de classe A, B, C, D e E
- Pelo fato que as redes da Internet variarem muito de tamanho



Endereços IP

Endereçamento “class-full”:

Classe

| | | | | |
|--|------|-------------------|------|---------------------------------|
| A | 0 | rede | host | 1.0.0.0 to 127.255.255.255 |
| $2^7 - 1$ (127) redes de grande porte com $2^{24} - 2$ hosts (16777214) | | | | |
| B | 10 | rede | host | 128.0.0.0 to 191.255.255.255 |
| 2^{14} (16384) redes com $2^{16} - 2$ hosts (65534) | | | | |
| C | 110 | rede | host | 192.0.0.0 to 223.255.255.255 |
| 2^{21} (2097152) redes pequenas com $2^8 - 2$ hosts (254) | | | | |
| D | 1110 | multicast address | | 224.0.0.0 to 239.255.255.255 |
|  | | | | |

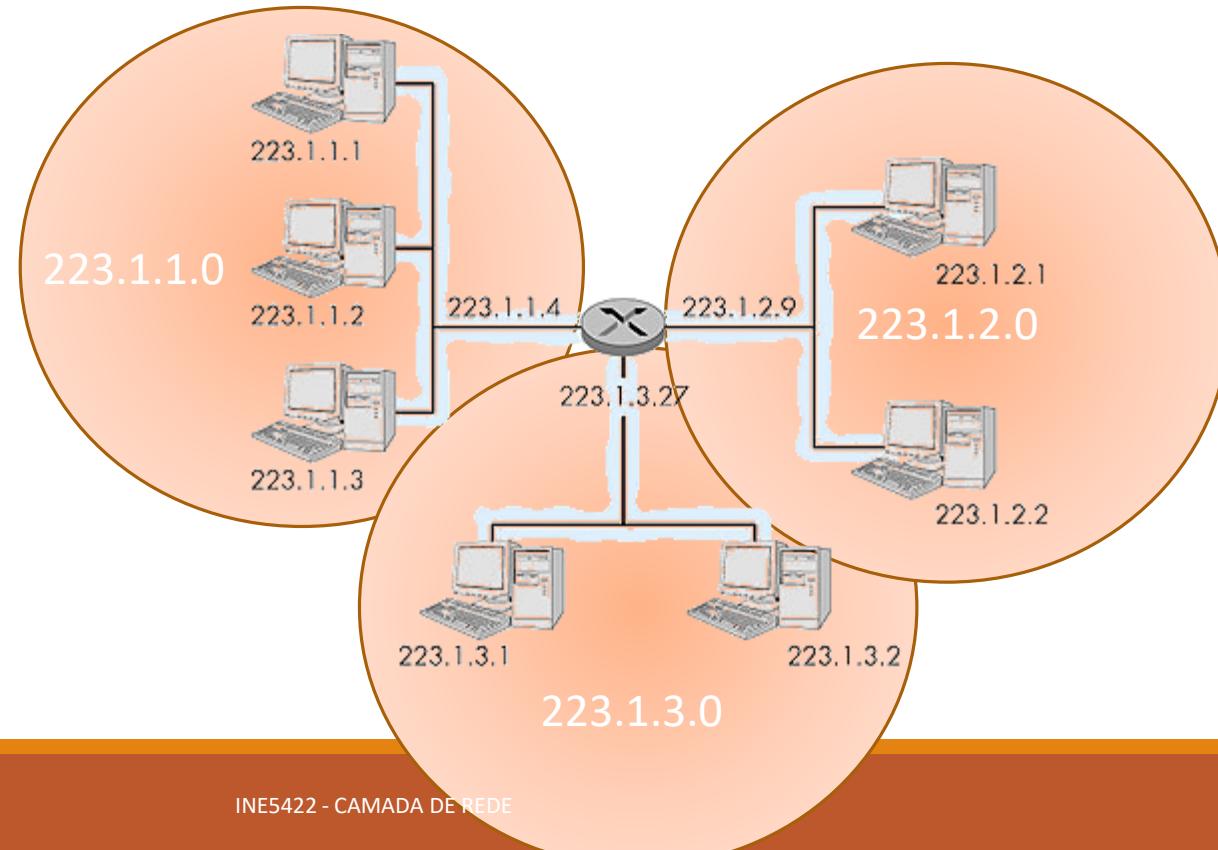
Endereços Especiais

| Prefixo | Sufixo | Exemplo | Tipo de endereço | Propósito |
|-----------|-----------|-----------------|--------------------|------------------------------------|
| Todos 0's | Todos 0's | 0.0.0.0 | Este computador | Usado durante o boot |
| Rede | Todos 0's | 200.200.200.0 | Rede | Identifica a rede |
| Rede | Todos 1's | 200.200.200.255 | Broadcast direto | Broadcast para uma rede específica |
| Todos 1's | Todos 1's | 255.255.255.255 | Broadcast limitado | Broadcast na rede local |
| 127 | Qualquer | 127.0.0.0 | Loopback | Identifica o próprio host |

Endereçamento IP

Como Roteadores e Hosts são ligados a rede

- Endereços IP são associados às interfaces
- Endereços IP podem também identificar uma rede
- Campo de host com todos bits iguais a 0



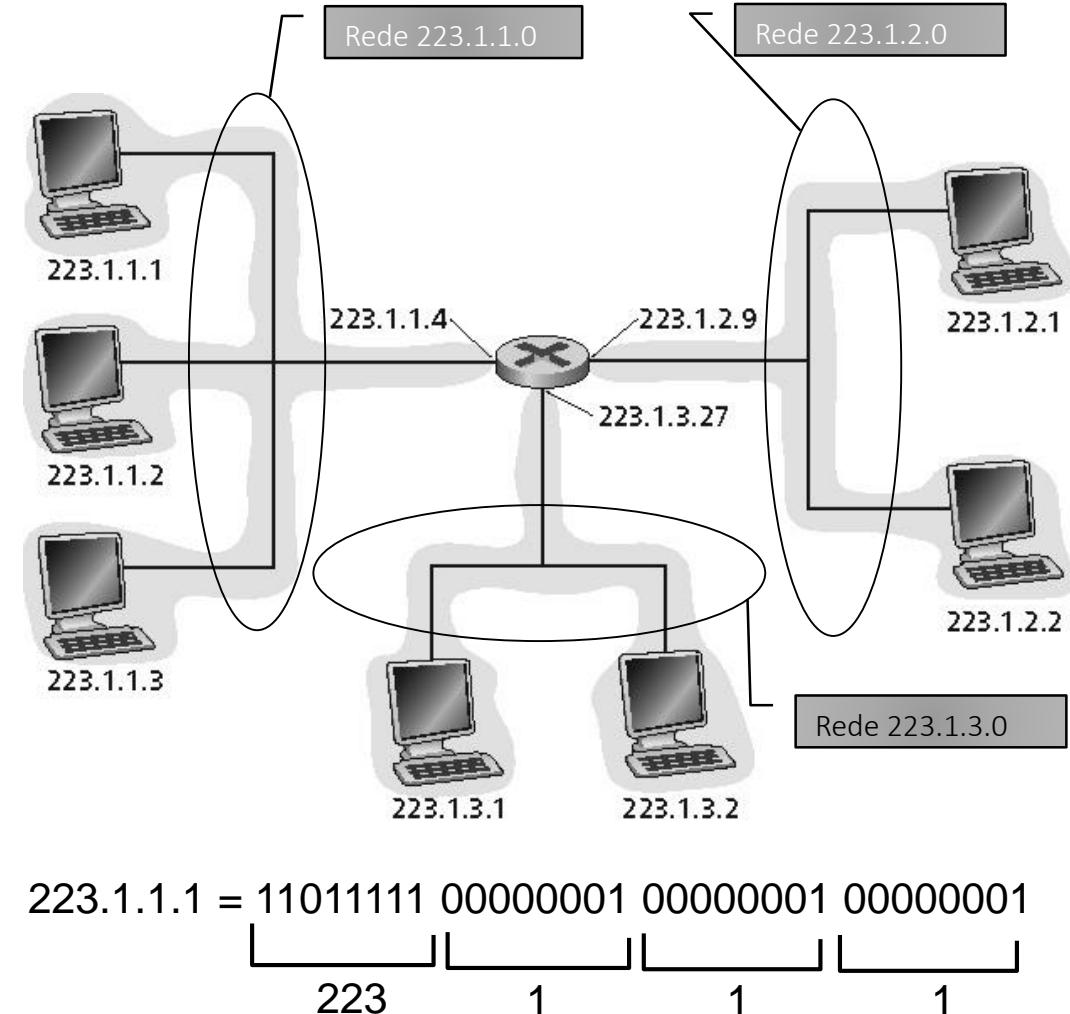
Endereçamento “class-full”

Endereço IP:

- Parte rede (bits mais significativos)
- Parte host (bits menos significativos)

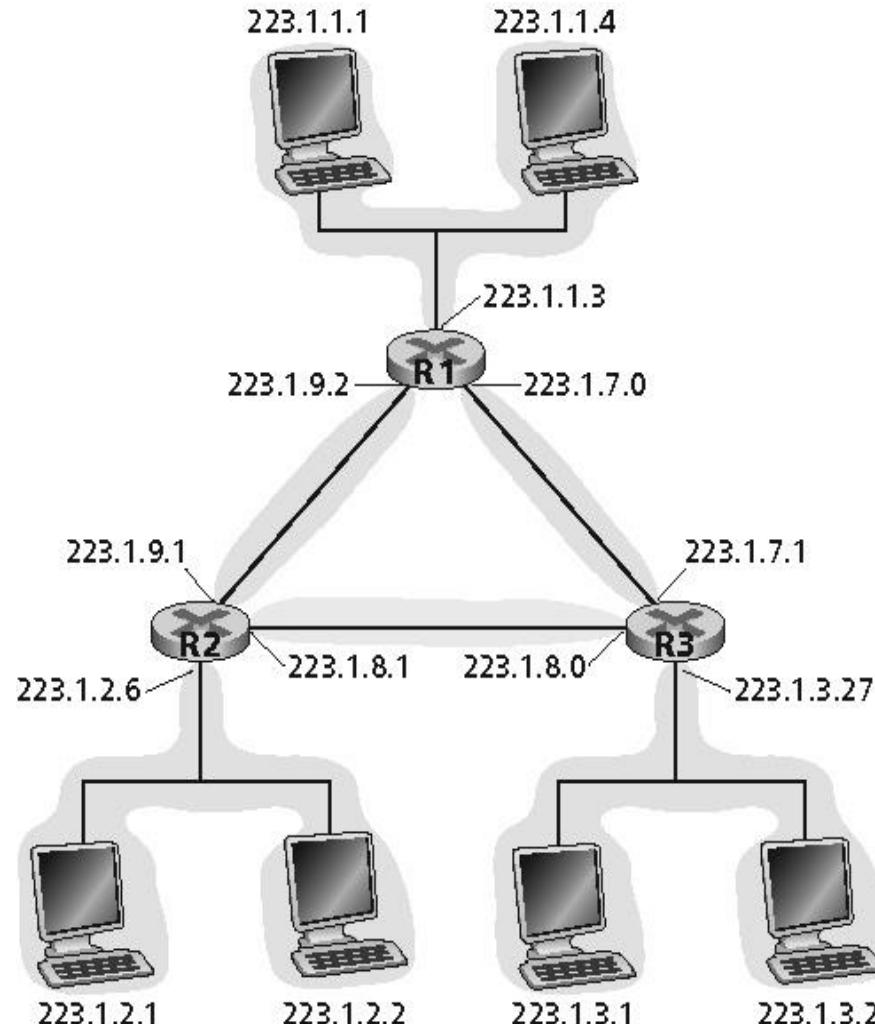
O que é uma rede? (da perspectiva de endereço IP)

- Dispositivos com interface com o mesma parte rede do endereço IP
- Pode alcançar fisicamente outro dispositivo sem intervenção do roteador



Endereçamento “class-full”

Quantas redes?



Pontos Importantes

Endereçamento IP

- Endereçamento horizontal e hierárquico
- Endereçamento class full

CAP 6. CAMADA DE REDE

AULA 2: ENDEREÇAMENTO IP (CIDR) E DHCP

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

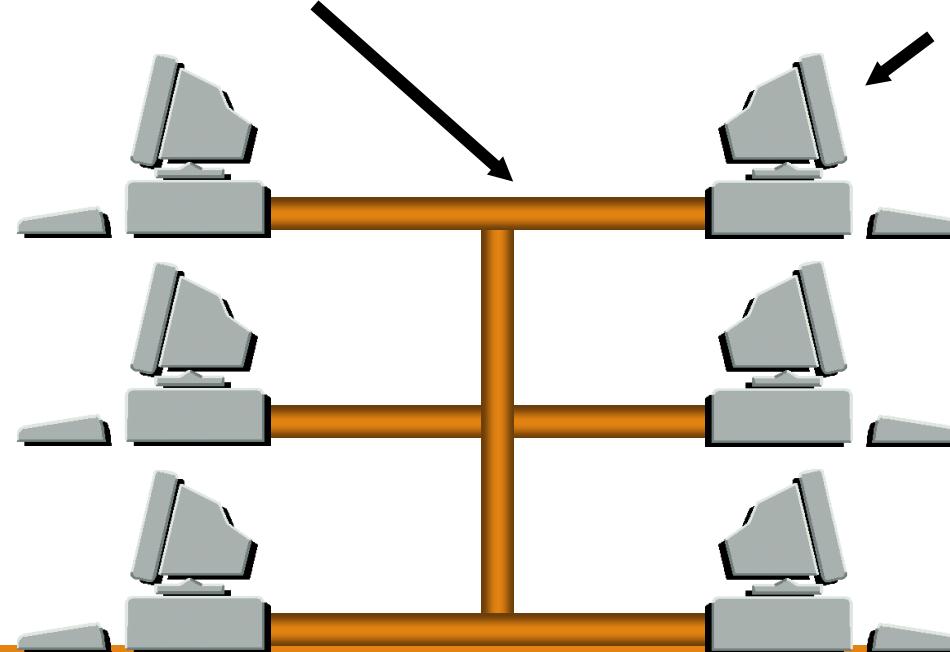
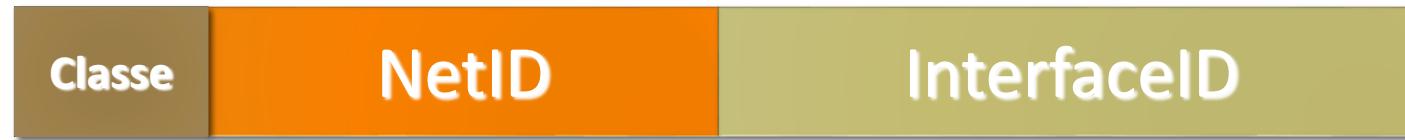
ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

Endereçamento IPv4

Endereçamento “class-full”:

- Redes de classe A, B, C, D e E
- Pelo fato que as redes da Internet variarem muito de tamanho



Endereços IP

Endereçamento “class-full”:

Classe

| | | | |
|---|----------|-------------------|---------------------------------|
| A | 0 rede | host | 1.0.0.0 to 127.255.255.255 |
| $2^7 - 1$ (127) redes de grande porte com $2^{24} - 2$ hosts (16777214) | | | |
| B | 10 rede | host | 128.0.0.0 to 191.255.255.255 |
| 2^{14} (16384) redes com $2^{16} - 2$ hosts (65534) | | | |
| C | 110 rede | host | 192.0.0.0 to 223.255.255.255 |
| 2^{21} (2097152) redes pequenas com $2^8 - 2$ hosts (254) | | | |
| D | 1110 | multicast address | 224.0.0.0 to 239.255.255.255 |
| 32 bits | | | |

Endereçamento “class-full”

Problemas do endereçamento “class-full”

- Com o crescimento de uma empresa o números de hosts possíveis de uma classe pode ser insuficiente
 - Se uma empresa tiver mais de 254 hosts e tiver um endereço classe C?
- Desperdício de blocos de endereços
 - Uma rede de Classe B aloca endereços para 65K hosts, mesmo se só existem 2000 hosts naquela rede

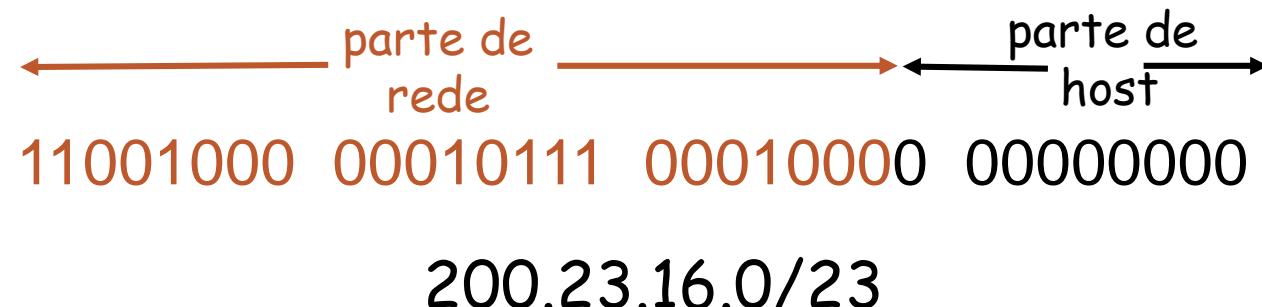
Endereçamento IP: CIDR

Endereçamento “Classfull”:

- Uso ineficiente do espaço de endereçamento, exaustão do espaço de endereços

CIDR: classless interdomain routing

- A porção de endereço de rede tem tamanho arbitrário
- Formato do endereço: A.B.C.D/x, onde x é o número de bits na parte de rede do endereço



Endereçamento IP: CIDR com a rede wireless.ufsc.br

Endereço IP de uma interface:

- 150.162.147.188
- Máscara de sub-rede: 255.255.254.0 (/23) => 23 bits iniciais identificam a rede e o restante a interface de rede (host)

Qual é o endereço da rede wireless.ufsc.br?

- 150.162.10010011.188/23 => endereço de uma interface
- 150.162.10010010.0 => endereço da rede tem todos os bits identificado a interface zerados
- 150.162.146.0 é o endereço da rede

Broadcast na rede wireless.ufsc.br

- Broadcast limitado: 255.255.255.255
- Broadcast direto: todos os bits da parte de host são setados:
 - 150.162.10010011.255 => 150.162.147.255

Atribuindo endereços

Como um host obtém seu endereço IP?

- Endereço de rede é fixo para uma rede
- Existem duas formas para atribuir um endereço de host

Configuração Manual

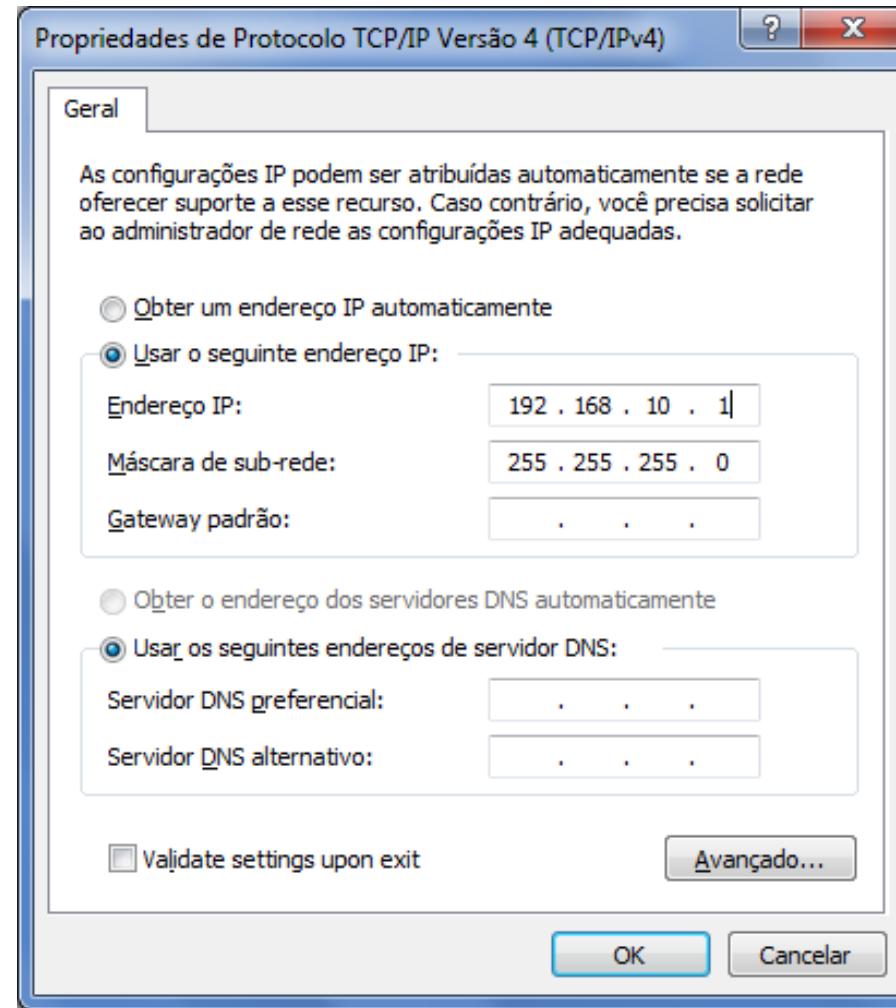
- O endereço IP é configurado no computador pelo administrador do sistema

Uso do DHCP

- Dynamic Host Configuration Protocol (DHCP)
 - Um servidor DHCP na rede recebe pedidos DHCP de um cliente e aloca um endereço IP para o cliente

Atribuindo endereços

Configuração Manual



DHCP

DHCP: Dynamic Host Configuration Protocol (RFC 2131)

- é um protocolo que oferece configuração dinâmica de terminais
 - com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.
 - é o sucessor do BOOTP.
 - DHCP utiliza UDP e a porta 67

Baseia-se no modelo cliente-servidor:

- Um cliente solicita informações de configuração (endereço IP, máscara de rede, gateway, servidores DNS,...)
- Servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede
 - Mais de um por rede (aumento da confiabilidade)

DHCP

Mantém pool de endereços

- Pool de endereços (ex: 192.168.1.20 até 192.168.1.254) disponíveis para “alugar” por um determinado período de tempo (lease time) para os clientes

O tempo do “alocação” dos endereços é configurável

- Se o tempo de alocação do endereço for muito longo...
 - ... faz com que o endereço que foi alocado para o cliente esteja impossibilitado de ser usado por outro host nesse período de tempo
- Se o tempo de alocação do endereço for muito curto...
 - ... faz com que o cliente tenha que solicitar com frequência a “renovação” do alocação

Para configurar o lease time

- deve ser levado em consideração a quantidade de hosts que a rede possui e o quanto dinâmico é o ambiente

DHCP

Ilustração de informações obtidas por um cliente DHCP

- Comando ipconfig /all (no command do windows)

DHCP

Ilustração de informações obtidas por um cliente DHCP

- Comando ipconfig /all (no command do windows)

```
Adaptador Ethernet Ethernet:  
  
Sufixo DNS específico de conexão. . . . . : inf.ufsc.br  
Descrição . . . . . : Realtek PCIe GbE Family Controller  
Endereço Físico . . . . . : 98-83-89-73-90-9F  
DHCP Habilitado . . . . . : Sim  
Configuração Automática Habilitada. . . . . : Sim  
Endereço IPv6 de link local . . . . . : fe80::880d:9b1a:db82:83bb%11(Preferencial)  
Endereço IPv4. . . . . : 150.162.58.204(Preferencial)  
Máscara de Sub-rede . . . . . : 255.255.254.0  
Concessão Obtida. . . . . : quarta-feira, 6 de novembro de 2024 12:44:09  
Concessão Expira. . . . . : quarta-feira, 6 de novembro de 2024 18:44:09  
Gateway Padrão. . . . . : 150.162.59.254  
Servidor DHCP . . . . . : 150.162.59.253  
IAID de DHCPv6. . . . . : 43549577  
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-21-4D-B3-C7-98-83-89-73-90-9F  
Servidores DNS. . . . . : 150.162.1.33  
                                150.162.2.33  
NetBIOS em Tcpip. . . . . : Habilitado  
  
Adaptador de Rede sem Fio Wi-Fi:  
  
Sufixo DNS específico de conexão. . . . . : wireless.ufsc.br  
Descrição . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter  
Endereço Físico . . . . . : 98-83-89-8E-3D-47  
DHCP Habilitado . . . . . : Sim  
Configuração Automática Habilitada. . . . . : Sim  
Endereço IPv4. . . . . : 200.135.75.205(Preferencial)  
Máscara de Sub-rede . . . . . : 255.255.254.0  
Concessão Obtida. . . . . : terça-feira, 5 de novembro de 2024 15:05:24  
Concessão Expira. . . . . : quarta-feira, 6 de novembro de 2024 12:57:08  
Gateway Padrão. . . . . : 200.135.75.254  
Servidor DHCP . . . . . : 10.254.254.254  
Servidores DNS. . . . . : 150.162.1.1  
                                150.162.2.2  
NetBIOS em Tcpip. . . . . : Habilitado
```

DHCP

Lease Life Cycle (ciclo de vida de alocação)

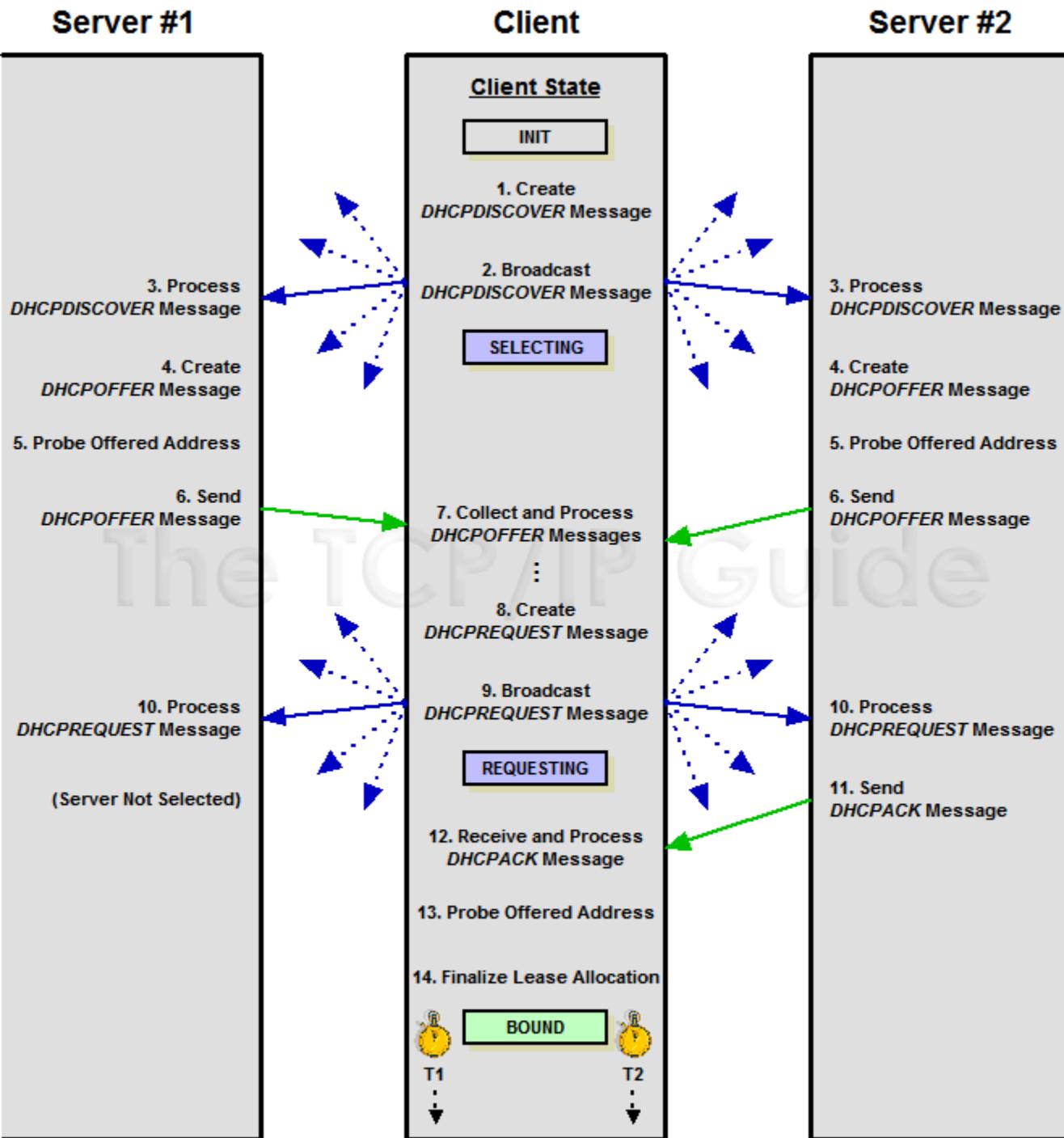
- Alocação (allocation):
 - O cliente não possui um endereço e então faz a requisição por alocação
- Re-alocação (reallocation):
 - Se o cliente já possui um endereço alocado, quando ele ligar ou reinicializar o host, ele irá contatar o servidor para confirmar a alocação
- Renovação (renewal):
 - Depois que um certo período do lease time tiver passado, o cliente contata o servidor para renovar a locação
- Liberação (release):
 - O cliente pode decidir a qualquer momento que não deseja mais utilizar o endereço que lhe foi alocado, e pode encerrar a locação

DHCP

Alocação (allocation) – figura no próximo slide

- Cliente envia uma mensagem broadcast “DHCP discover” para encontrar servidores DHCP
- Caso haja um servidor DHCP na rede (ou até mais de um) o mesmo responde com uma mensagem “DHCP offer”, ofertando alocação de um endereço para o cliente
- Entre a(s) oferta(s) recebidas(s) – de acordo com o número de servidores que responderam – o cliente solicita uma das ofertas (normalmente a primeira recebida – depende da implementação do sistema operacional) com uma mensagem “DHCP request”
- O servidor que recebeu a requisição pela oferta então confirma a alocação através da mensagem “DHCP ack”

DHCP



Re-alocação (reallocation)

- Se um cliente é inicializado e ele já possui o alocação de um endereço, ele não precisa passar por todo o processo de alocação
- O cliente envia uma mensagem para encontrar o servidor que possui as informações sobre sua alocação “DHCP request”
- O servidor responde ao cliente confirmado que o alocação ainda é válido “DHCP ack”

DHCP

Renovação (renewal)

- Cada cliente tem associado com seu endereço um renewal timer (T1), normalmente setado para 50% do tempo do alocação
- Quando T1 esgotar, o cliente tentará renovar seu alocação com seu servidor DHCP antes que o mesmo expire
- Caso não consiga efetuar a renovação até que o tempo do alocação expire, o cliente entrará no processo de rebinding
 - Aqui, irá disparar um broadcast para ver se algum servidor será capaz de renovar seu endereço atual
- Por fim, caso nenhum servidor faça a renovação, o cliente terá que refazer o processo de alocação

DHCP

Liberação (release)

- Por alguma razão, um usuário pode decidir terminar com o alocação de um determinado IP
- O cliente envia então uma mensagem DHCPRelease ao servidor DHCP que mantém seu contrato
- O servidor libera o endereço IP para que o mesmo possa então ser utilizado por outro cliente

DHCP

Configuração Manual x Configuração Automática

Configuração Manual

Endereço IP atribuído manualmente em cada computador

Possibilidade de atribuir endereços inválidos ou conflitantes

Sobrecarga de trabalho aos administradores da rede

Pouco amigável com usuários móveis

Configuração Automática

Endereço IP atribuído dinamicamente para cada computador

Cientes sempre terão configurações de endereçamento corretas

Diminui a sobrecarga de trabalho dos administradores de rede / Administração centralizada

Mais amigável com usuários móveis

Pontos Importantes

Endereçamento IP

- Entender endereçamento sem classes e máscaras de sub-rede
- Conhecer o protocolo DHCP

CAP 6. CAMADA DE REDE

AULA 3: MAPEAMENTO PARA ENDEREÇOS DE LAN E ATRIBUINDO BLOCOS DE ENDEREÇOS

INE5422 Redes De Computadores II

Prof. Roberto Willrich (INE/UFSC)

[Roberto.Willrich@ufsc.Br](mailto:Roberto.Willrich@ufsc.br)

[Https://Moodle.Ufsc.Br](https://Moodle.Ufsc.Br)

Mapeamento de Endereços

Mapeamento do endereço de um host em um endereço de sub-rede (muitas vezes o endereço de enlace-Endereço Físico)

- Problema a ser resolvido pelo nível de rede

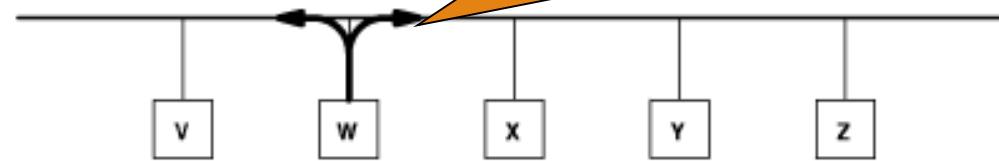
ARP (Address Resolution Protocol)

- Endereços IP: virtuais (software)
- Hardware não consegue localizar host utilizando o endereço IP
- ARP
 - Resolução de Endereço: mapear endereço físico para endereço lógico

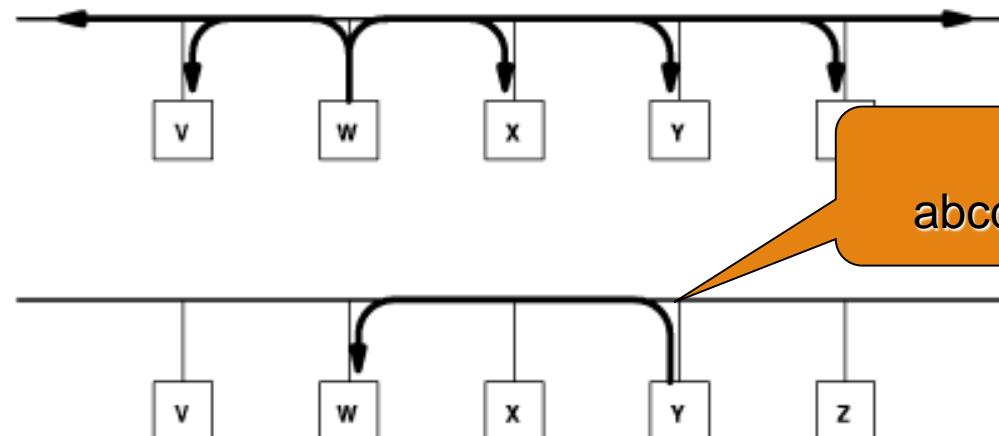
Como fazer ?

2) Troca de Mensagens.

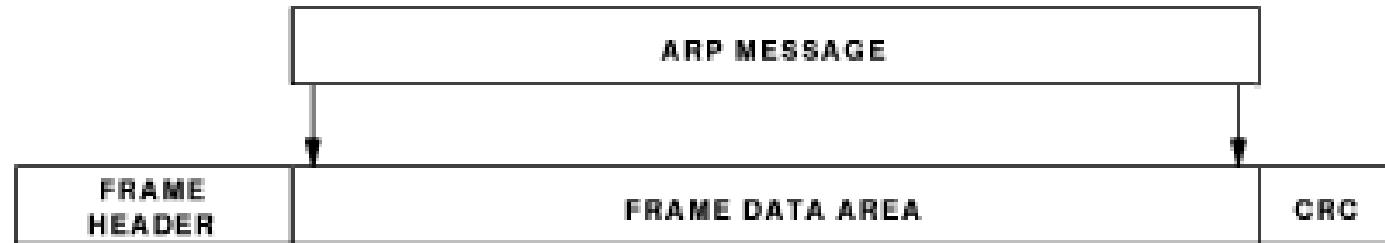
Qual é o endereço
Ethernet do Host
 $x.y.w.z$?



Sou eu
abcd:efgh:ijkl:mopq



Enviando uma mensagem ARP



Mensagem ARP encapsulada dentro de um quadro Ethernet

Mapeamento de Endereços

ARP define a tradução de endereços IP em endereços físicos ETHERNET:

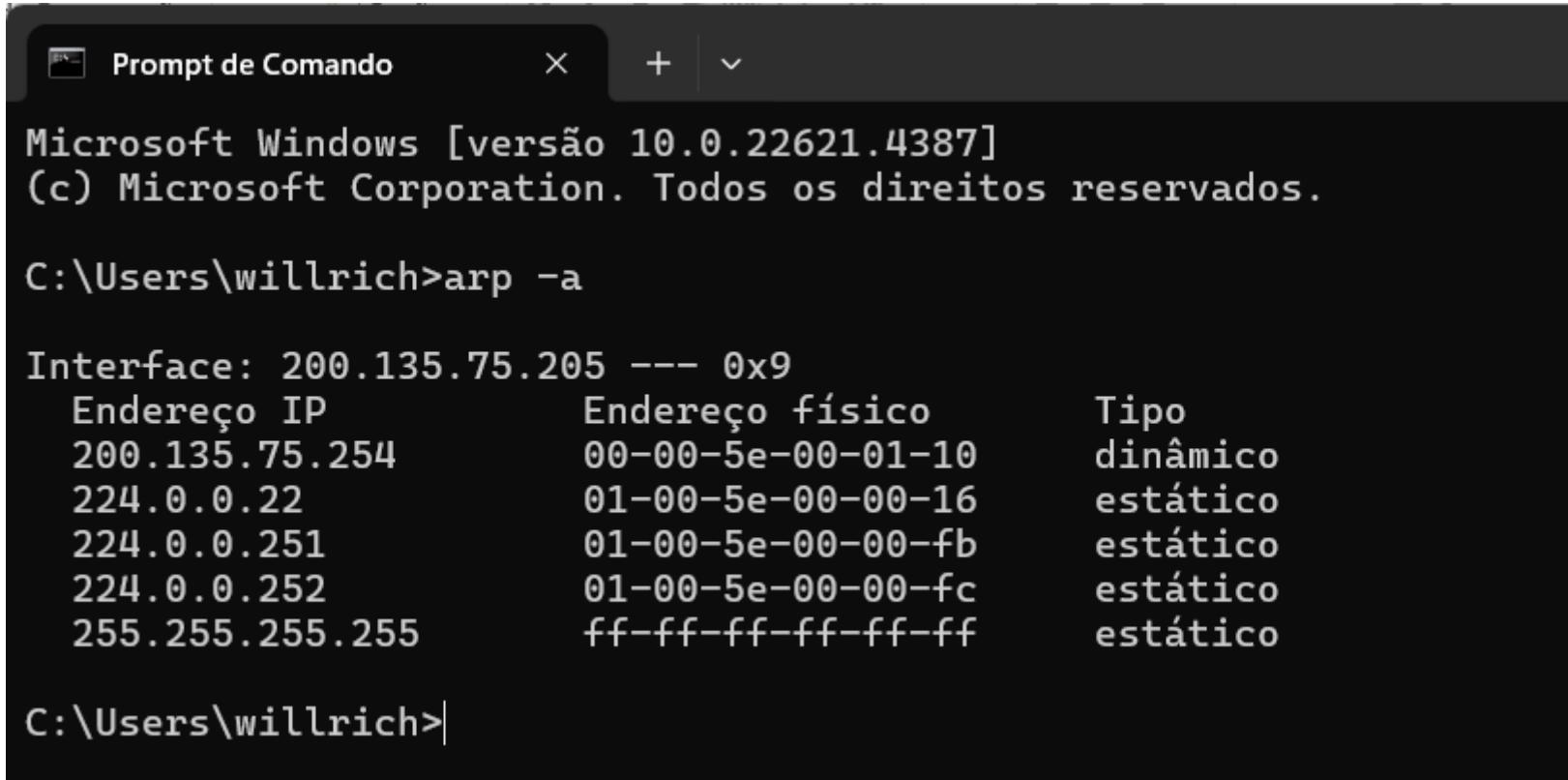
- Cada adaptador ETHERNET possui endereço único na LAN;
- ARP utiliza uma tabela de tradução:

| Endereço IP | Endereço Ethernet |
|---------------|-------------------|
| 150.162.60.60 | 08:00:20:11:FD:25 |
| 150.162.60.12 | 08:00:20:11:FD:25 |
| 150.162.60.50 | 08:00:20:11:FE:F9 |

- Se o endereço procurado não está na tabela, então difunde um pacote, para toda a rede física, perguntando pelo endereço;
- Se alguém responde, então o endereço é inserido na tabela.

Mapeamento de Endereços

1) Pesquisa em tabelas.



```
Prompt de Comando
Microsoft Windows [versão 10.0.22621.4387]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\willrich>arp -a

Interface: 200.135.75.205 --- 0x9
  Endereço IP        Endereço físico      Tipo
  200.135.75.254    00-00-5e-00-01-10  dinâmico
  224.0.0.22         01-00-5e-00-00-16  estático
  224.0.0.251        01-00-5e-00-00-fb  estático
  224.0.0.252        01-00-5e-00-00-fc  estático
  255.255.255.255   ff-ff-ff-ff-ff-ff  estático

C:\Users\willrich>
```

Atribuindo endereços

Obtendo um endereço de rede

- O administrador da rede da organização deve contactar a provedora de serviços internet (ISP)
 - Que poderia fornecer endereços a partir de um grande bloco de endereços que teria sido alocado para a ISP
- Se ISP tem alocado o bloco de endereço 200.23.16.0/20
 - ISP poderia dividir o bloco de endereço em 8 blocos menores de endereços para cada uma das organizações suportadas pela ISP
 - Bloco da ISP 11001000 00010111 00010000 00000000 200.23.16.0/20
 - Organização 0 11001000 00010111 00010000 00000000 200.23.16.0/23
 - Organização 1 11001000 00010111 00010010 00000000 200.23.18.0/23
 - Organização 2 11001000 00010111 00010100 00000000 200.23.20.0/23
 - ...
 - Organização 7 11001000 00010111 00011110 00000000 200.23.30.0/23

Atribuindo endereços

Como uma ISP obtém seu bloco de endereços?

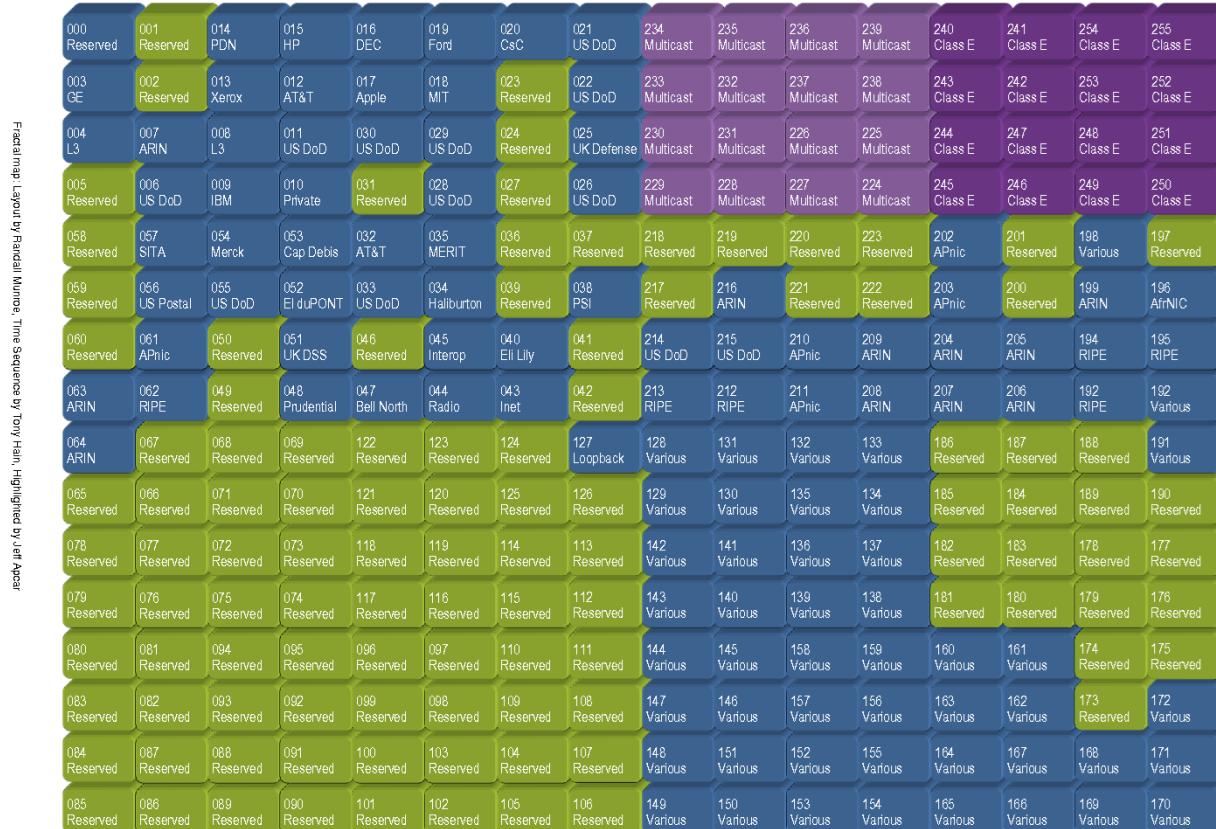
- Endereços IP são gerenciados pela Internet Corporation for Assigned Names and Numbers (ICANN)
 - Aloca não apenas endereços IP, mas também gerenciam servidores raiz DNS
- Atualmente endereços são gerenciados por registradores Internet regionais



Atribuindo endereços

ICANN aloca bloco de endereços para registradores Internet regionais

IPv4 Address Fractal Map Jan-2000



Atribuindo endereços

Alocação dos blocos IPv4:

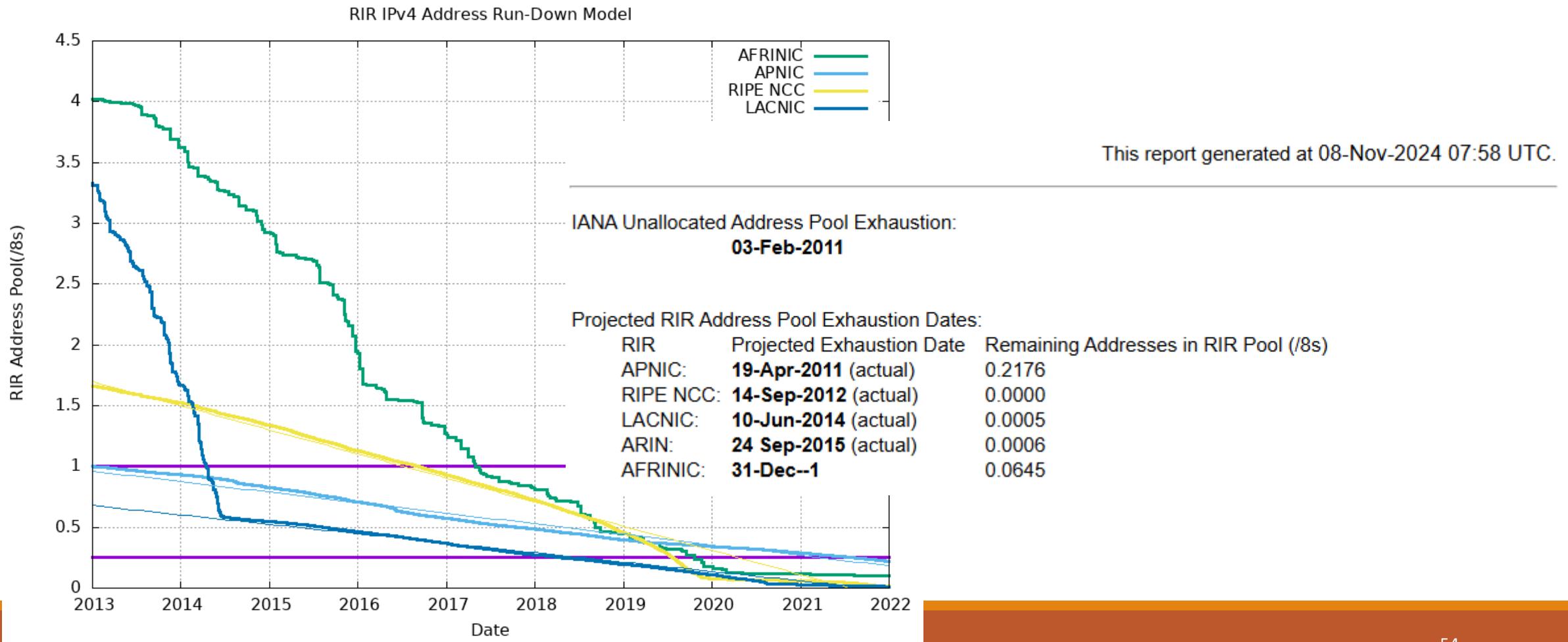
- <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

| Blocos de Endereços Reservados | | | |
|--------------------------------|--------------------|---|--------------------------|
| CIDR | Bloco de Endereços | Descrição | Referência |
| 0.0.0.0/8 | | Rede corrente (só funciona como endereço de origem) | RFC 1700 |
| 10.0.0.0/8 | | Rede Privada | RFC 1918 |
| 14.0.0.0/8 | | Rede Pública | RFC 1700 |
| 39.0.0.0/8 | | Reservado | RFC 1797 |
| 127.0.0.0/8 | | Localhost | RFC 3330 |
| 128.0.0.0/16 | | Reservado (IANA) | RFC 3330 |
| 169.254.0.0/16 | | Zeroconf | RFC 3927 |
| 172.16.0.0/12 | | Rede privada | RFC 1918 |
| 191.255.0.0/16 | | Reservado (IANA) | RFC 3330 |
| 192.0.2.0/24 | | Documentação | RFC 3330 |
| 192.88.99.0/24 | | IPv6 para IPv4 | RFC 3068 |
| 192.168.0.0/16 | | Rede Privada | RFC 1918 |
| 198.18.0.0/15 | | Teste de benchmark de redes | RFC 2544 |
| 223.255.255.0/24 | | Reservado | RFC 3330 |
| 224.0.0.0/4 | | Multicasts (antiga rede Classe D) | RFC 3171 |
| 240.0.0.0/4 | | Reservado (antiga rede Classe E) | RFC 1700 |
| 255.255.255.255 | | Broadcast | |

Atribuindo endereços

Blocos de Endereços IPv4 esgotados

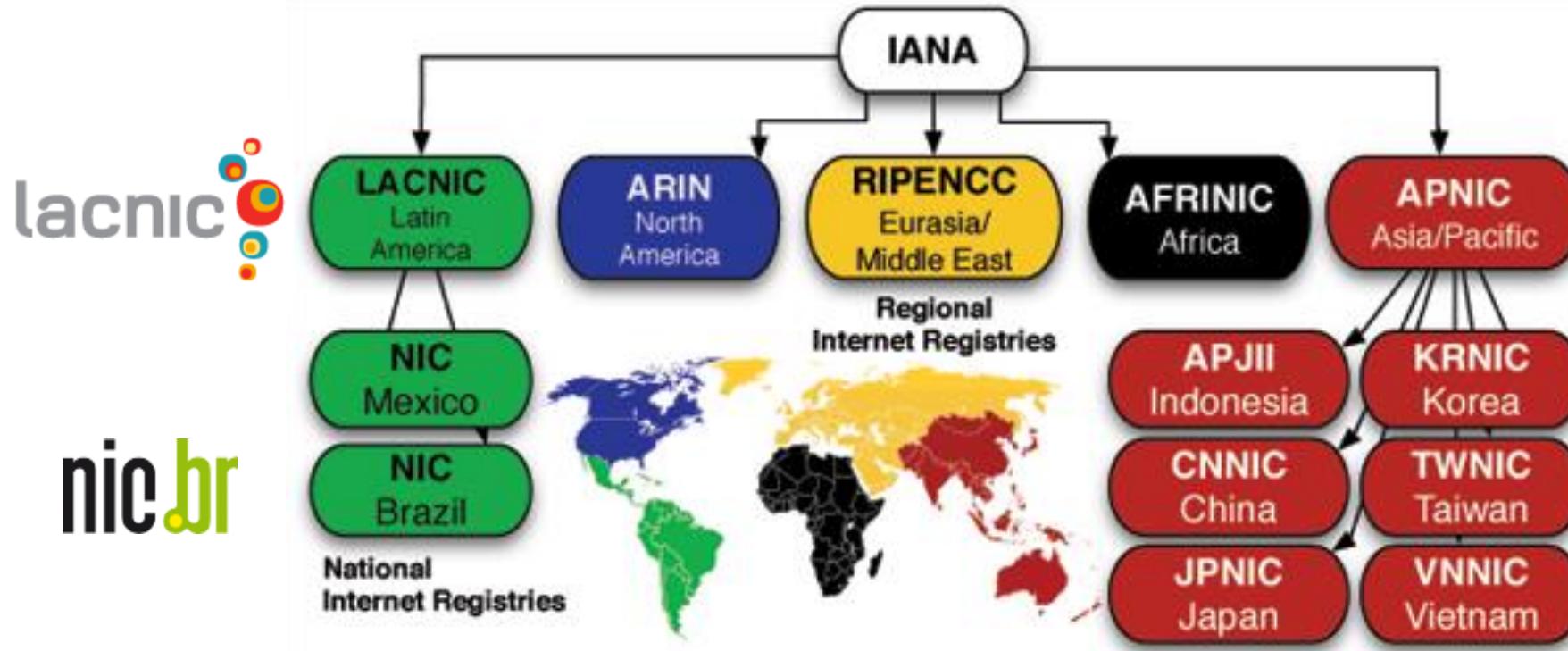
- <https://www.potaroo.net/tools/ipv4/>



Atribuindo endereços

Como um ISP obtém seus blocos de endereço IPv4?

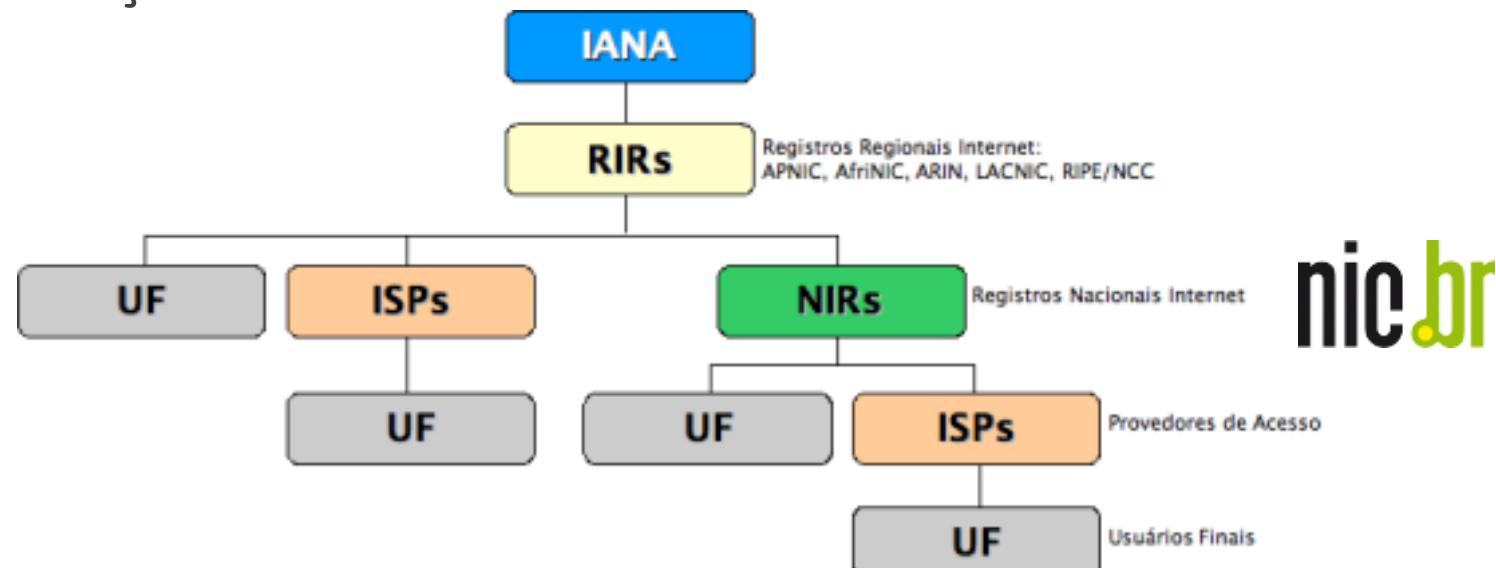
- Via a representação nacional do órgão regional



Atribuindo endereços

Como um ISP obtém seus blocos de endereço IPv4?

- Recursos de Numeração distribuídos pelo Registro.br:
 - ASN (Autonomous System Number)
 - Blocos de endereços IPv4
 - Regras em <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao>
 - Blocos de endereços IPv6



Atribuindo endereços

Custos para ISPs: <https://registro.br/tecnologia/numeracao/custos/>



| CATEGORIA | TAMANHO/PREFIXOS | CUSTO INICIAL/RENOVAÇÃO |
|-----------------|--|-------------------------|
| Nano | IPv4: menor que /22 | R\$ 3.060,00 |
| Micro | IPv4: menor que /20 | R\$ 5.100,00 |
| Small | IPv4: menor que /18 e/ou IPv6: menor igual que /32 | R\$ 10.710,00 |
| Small IPv6 Only | IPv4: nenhum bloco IPv6: menor igual que /32 | R\$ 4.590,00 |
| Medium | IPv4: menor que /16 e/ou IPv6: menor que /30 | R\$ 29.070,00 |
| Large | IPv4: menor que /14 e/ou IPv6: menor que /28 | R\$ 71.400,00 |
| X-Large | IPv4: menor que /12 e/ou IPv6: menor que /26 | R\$ 142.800,00 |
| 2X-Large | IPv4: menor que /11 | R\$ 229.500,00 |
| 2X-Large | IPv4: menor que 2/11 e/ou IPv6: menor que /24 | R\$ 331.500,00 |
| 3X-Large | IPv4: menor que 3/11 | R\$ 433.500,00 |

Atribuindo endereços

Custos para Usuário Final: <https://registro.br/tecnologia/numeracao/custos/>

| TAMANHO | CUSTO INICIAL | MANUTENÇÃO ANUAL |
|--|-----------------------------|------------------|
| IPv4: /24 até /22 e/ou IPv6: /48 até /35 | R\$ 12.750,00 | R\$ 3.060,00 |
| IPv6: maior que /35 até /32 | R\$ 25.500,00 cada /32 IPv6 | R\$ 3.060,00 |
| IPv6: menor que /30 | R\$ 29.070,00 | R\$ 29.070,00 |
| IPv6: menor que /28 | R\$ 71.400,00 | R\$ 71.400,00 |
| IPv6: menor que /26 | R\$ 142.800,00 | R\$ 142.800,00 |
| IPv6: menor que /24 | R\$ 331.500,00 | R\$ 331.500,00 |
| IPv6: menor que /22 | R\$ 535.500,00 | R\$ 535.500,00 |
| IPv6: menor que /20 | R\$ 943.500,00 | R\$ 943.500,00 |
| IPv6: menor que /19 | R\$ 1.759.500,00 | R\$ 1.759.500,00 |



Pontos Importantes

Protocolo ARP e obtendo blocos de endereços IP

- Entender os objetivos e funcionamento do protocolo ARP
- Entender como os blocos de endereçamento IP são atribuídos a ISPs e usuários finais

CAP 6. CAMADA DE REDE

AULA 4: NAT (NETWORK ADDRESS TRANSLATOR)

INE5422 Redes De Computadores II

Prof. Roberto Willrich (INE/UFSC)

Roberto.Willrich@ufsc.Br

<Https://Moodle.Ufsc.Br>

NAT (Network Address Translator)

Tecnologia que permite ligar uma rede com endereços IP privados (não utilizáveis na Internet) à Internet através de um servidor de NAT

- Contornar o problema de falta de números IP
- Traduz endereço válido em privado e vice-versa

Endereços Privados

- Faixas de endereços privados são definidas na RFC 1597:
 - 10.0.0.0 -> 10.255.255.255
 - 172.16.0.0 -> 172.31.255.255
 - 192.168.0.0 -> 192.168.255.255
- Qualquer empresa pode utilizar estas faixas

NAT (Network Address Translator)

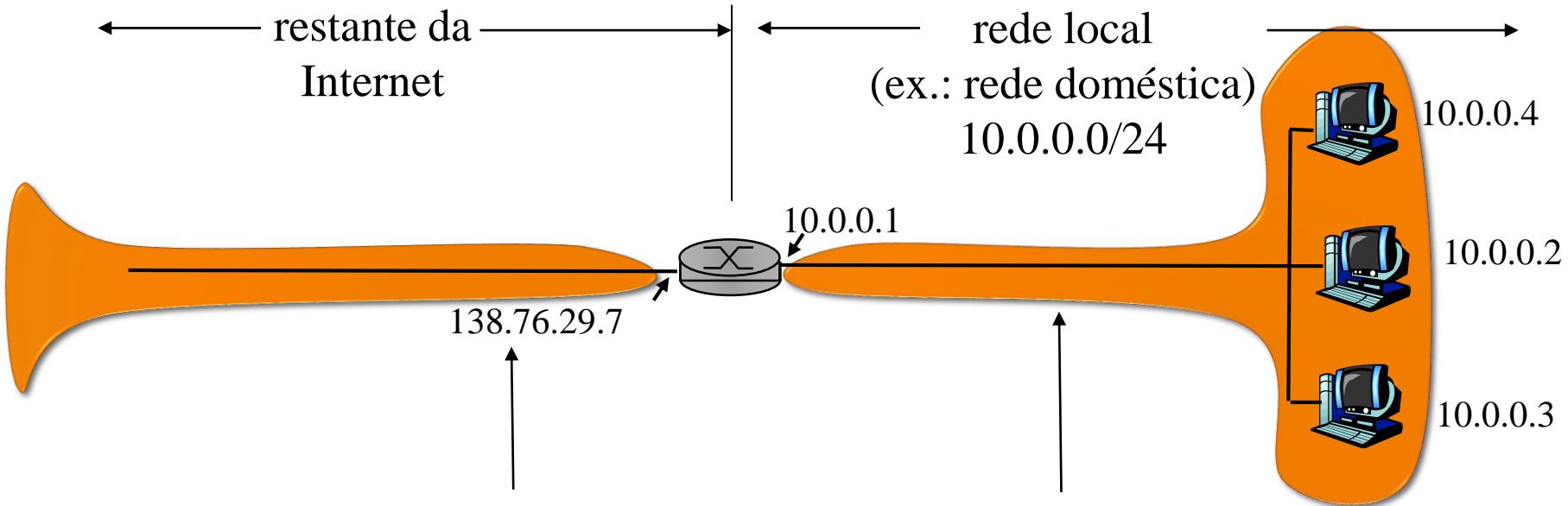
Exemplo de uso

- Rede com 100 computadores com esquema de endereçamento 10.10.0.0/255.255.0.0
 - Pode ter acesso à Internet usando um único endereço IP válido: o endereço IP da interface externa do NAT.
 - Uma grande economia de endereços IP!

Duas formas de tradução

- NAT Básico: a tradução simples de endereço IP global para endereço IP privado (sem mapeamento de portas)
- NAPT/PAT (Port Address Translation): Envolve a tradução de endereços IP e de número de portas

NAT: Exemplo



todos os datagramas que **saem** da rede local possuem o **mesmo** e único endereço IP do NAT de origem:
138.76.29.7,
números diferentes de portas de origem

datagramas com origem ou destino nesta rede possuem endereço 10.0.0.0/24 para origem, destino (usualmente)

NAT (Network Address Translator)

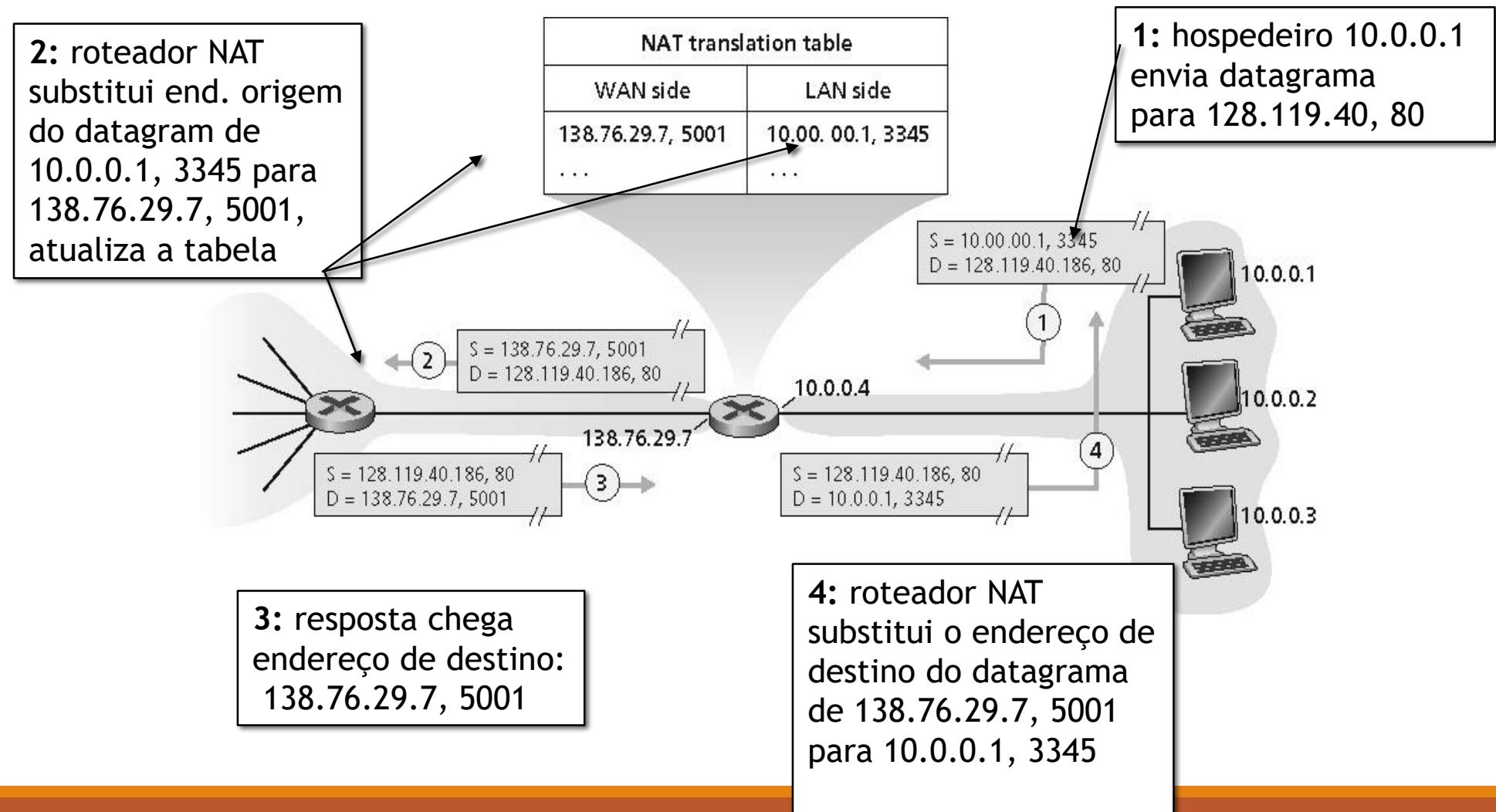
Servidor NAT

- Pode-se usar um equipamento específico (router com capacidade de NAT), um servidor Linux, ou uma máquina Windows com ICS (Internet Connection Sharing) ou outro software como Wingate ou Winroute

Configuração

- IP da interface interna: 10.10.0.1 ou 192.168.0.1 ou outro reservado
- IP da interface externa: Um ou mais endereços válidos na Internet
 - obtidos a partir da conexão com o provedor de Internet

NAPT



NAPT

Quando um cliente acessa a Internet

- Pacote contém o endereço IP da rede interna.
 - Ex.: 10.10.0.10.
 - Pacote não pode ser enviado à Internet pois endereço é privado

Servidor NAT:

- Datagramas que saem:
 - Substitue (endereço IP de origem, porta #) de cada datagrama para (endereço IP do NAT, nova porta #)
 - Clientes/servidores remotos responderão usando (endereço IP do NAT, nova porta #) como endereço de destino.
- Mantem a tabela de tradução do NAT
 - Cada (endereço IP de origem, porta #) para o par de tradução (endereço IP do NAT, nova porta #).
- Datagramas que chegam
 - substitue (endereço IP do NAT, nova porta #) nos campos de destino de cada datagrama pelos correspondentes (endereço IP de origem, porta #) armazenados da tabela NAT

NAPT

Tarefas e comportamentos

- Modificar o endereço IP de acordo com a tabela NAT
- Modificar o checksum do IP e TCP
- Modificar pacotes ICMPs
- Modificações nos campos do FTP, NetBIOS sobre TCP/IP, SNMP, DNS, Kerberos, X-Windows, SIP, H.323, IKE...)
- Pacotes emitidos e recebidos deveriam não ter ciência da existência do NAT

NAPT

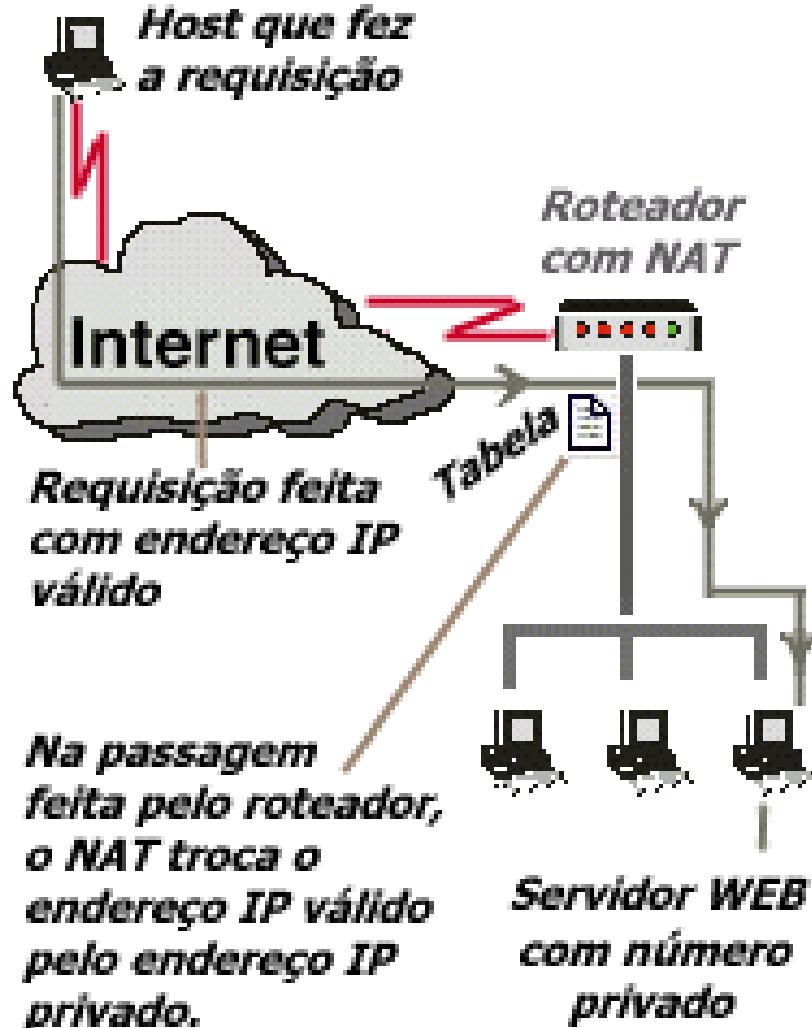
Campo número de porta com 16 bits:

- 65.535 conexões simultâneas com um único endereço de LAN

NAT é controverso:

- Roteadores deveriam processar somente até a camada 3
 - Violação do argumento fim-a-fim
- A possibilidade de NAT deve ser levada em conta pelos desenvolvedores de aplicações, ex., aplicações P2P
- A escassez de endereços deveria ser resolvida pelo IPv6

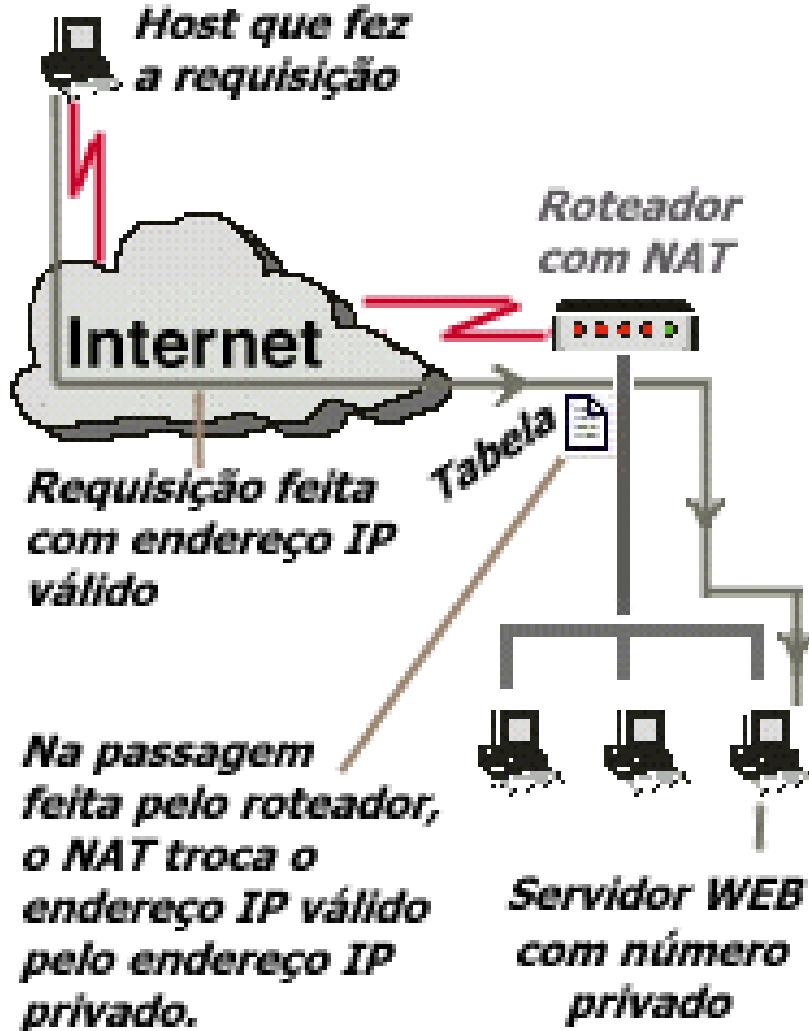
NAT (Network Address Translator)



Traduções estáticas

- Úteis quando disponibilizamos serviços na rede interna, como exemplo, um site Web
- quando o pedido de conexão chega ao roteador, o NAT consulta a tabela de endereços e transcreve para o IP interno correspondente, permitindo assim, que seja possível fazer uma conexão no sentido da Internet para a rede interna.

NAT (Network Address Translator)



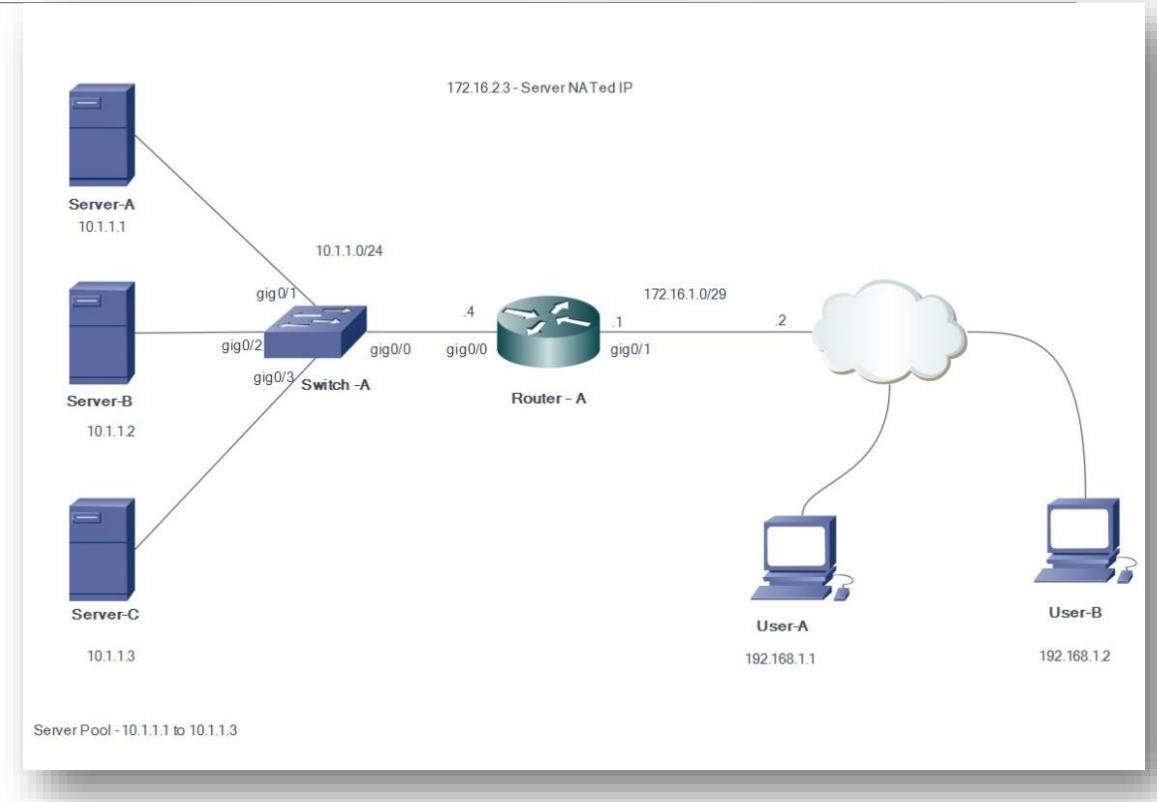
Traduções Dinâmicas

- úteis quando se pretende dar acesso aos computadores no sentido da rede corporativa para Internet
- Endereço válido pode ser único ou uma faixa de endereços
- No retorno do pedido: NAT consulta a tabela de traduções e responde a máquina que fez a requisição.

NAT (Network Address Translator)

Outras aplicações

- Balanceamento de carga
 - Uso de um IP global representando um “servidor virtual”
 - Na forma de várias máquinas com IPs locais
 - Servidor NAT traduz endereço global em local de acordo com um algoritmo de distribuição
- Alta disponibilidade
 - Se uma máquina falhar, o servidor virtual ainda continua operando (com os outros servidores)



Pontos Importantes

NAT

- Entender seu funcionamento

CAP 6. CAMADA DE REDE

AULA 5: PROTOCOLO IP E SEUS SERVIÇOS

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

Protocolo IP: Serviços

Protocolo IP não garante confiabilidade (não possui controle de perda de pacotes)

- Não é usado reconhecimentos
- Possui checagem de pacotes que chegam usando checksum do cabeçalho
 - Garante que as informações usadas pelos roteadores estão corretas

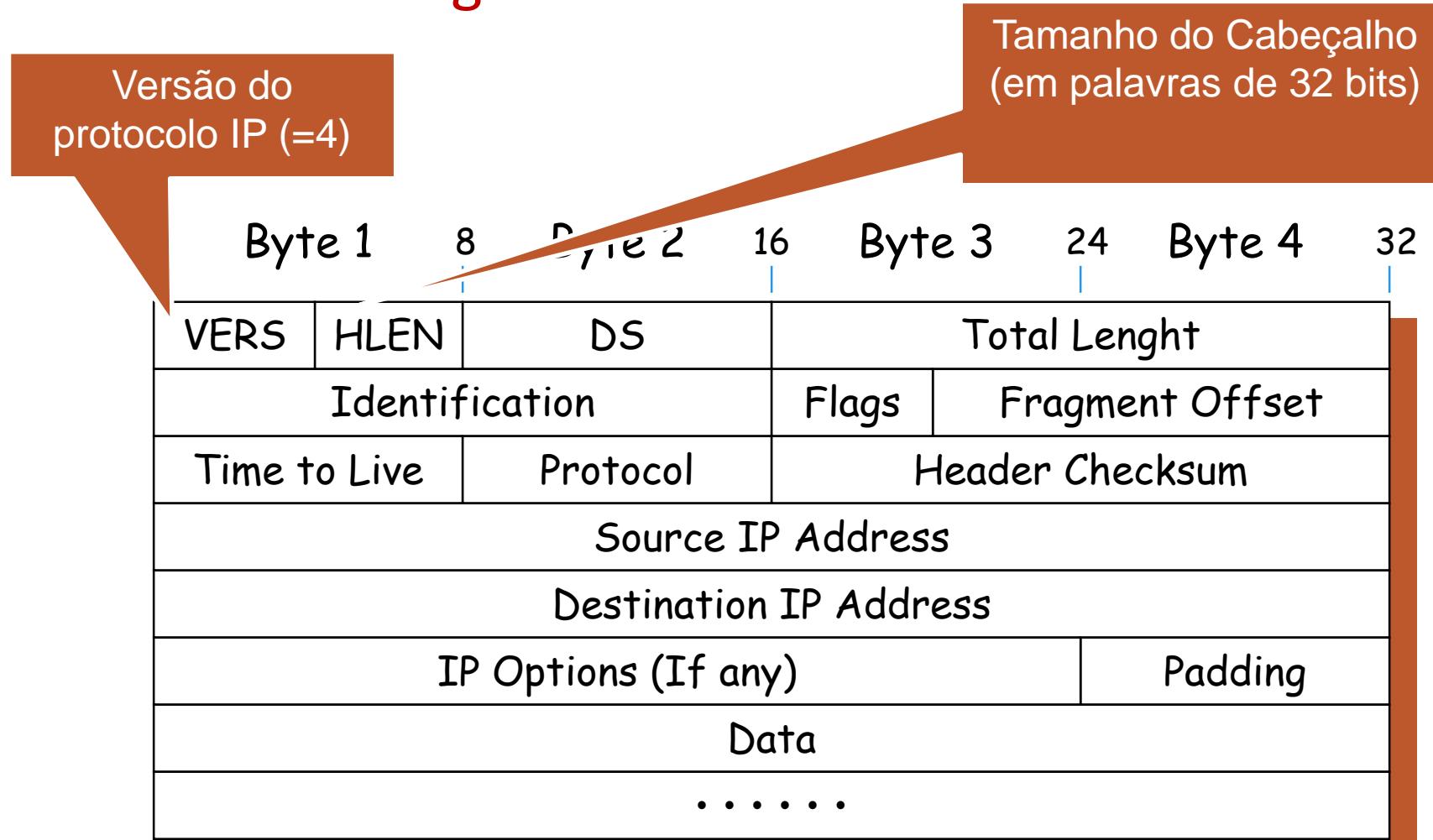
Não existe controle de fluxo e de congestionamento

Fornece um serviço de segmentação e remontagem de datagramas longos

- Para que eles possam ser transferidos através de redes onde o tamanho máximo (MSS) permitido para os pacotes é pequeno

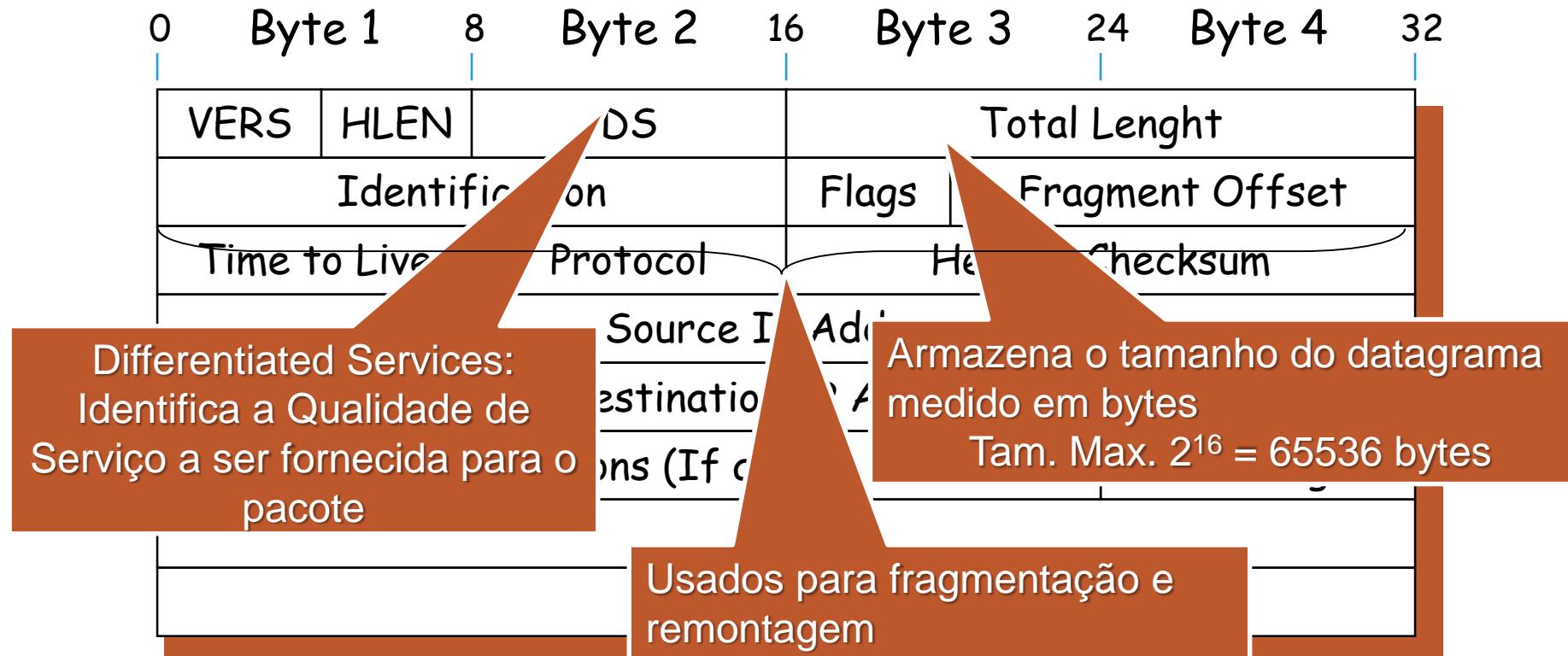
Formato do Datagrama IP

Formato do Datagrama IP



Formato do Datagrama IP

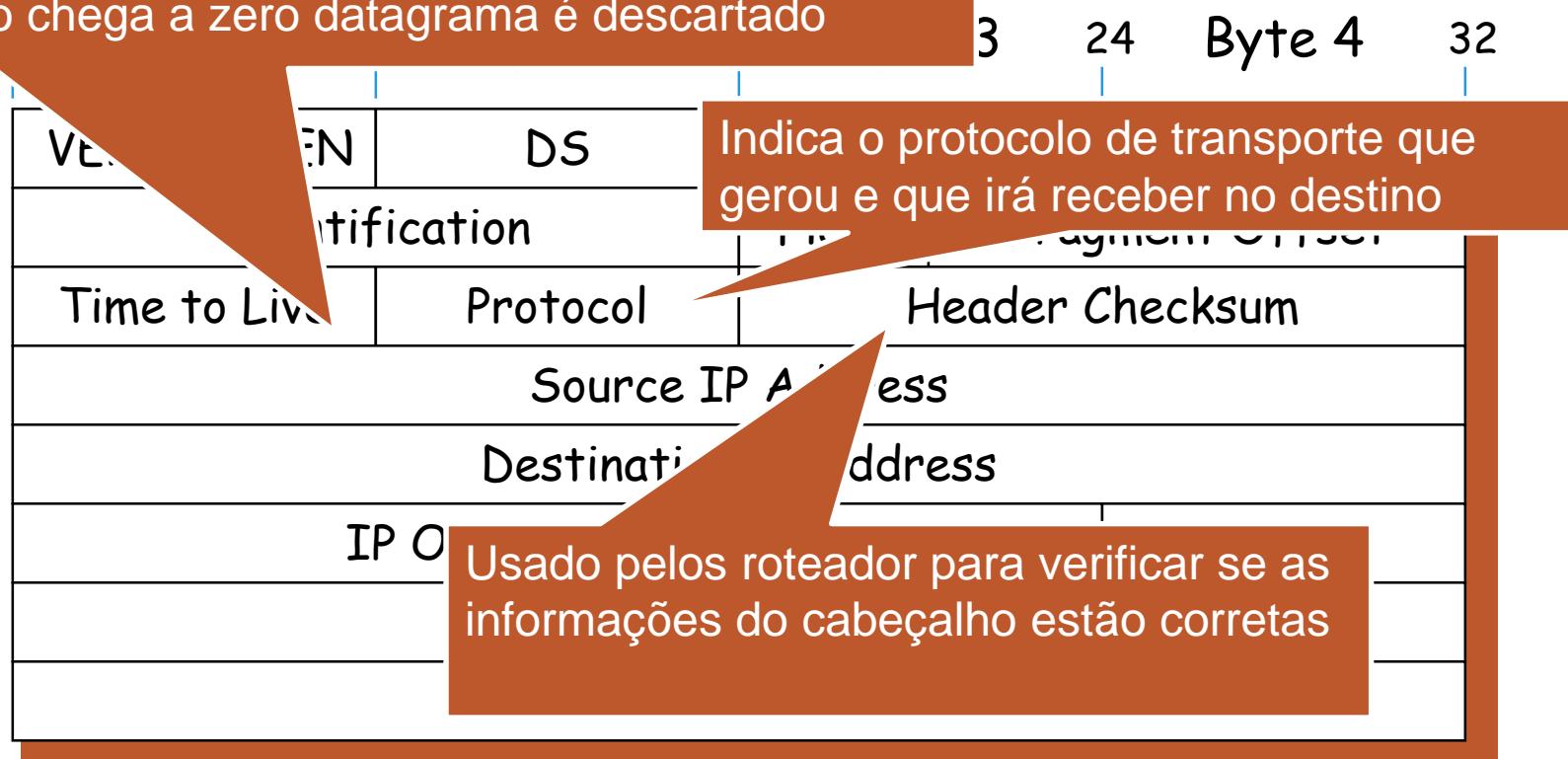
Formato do Datagrama IP



Formato do Datagrama IP

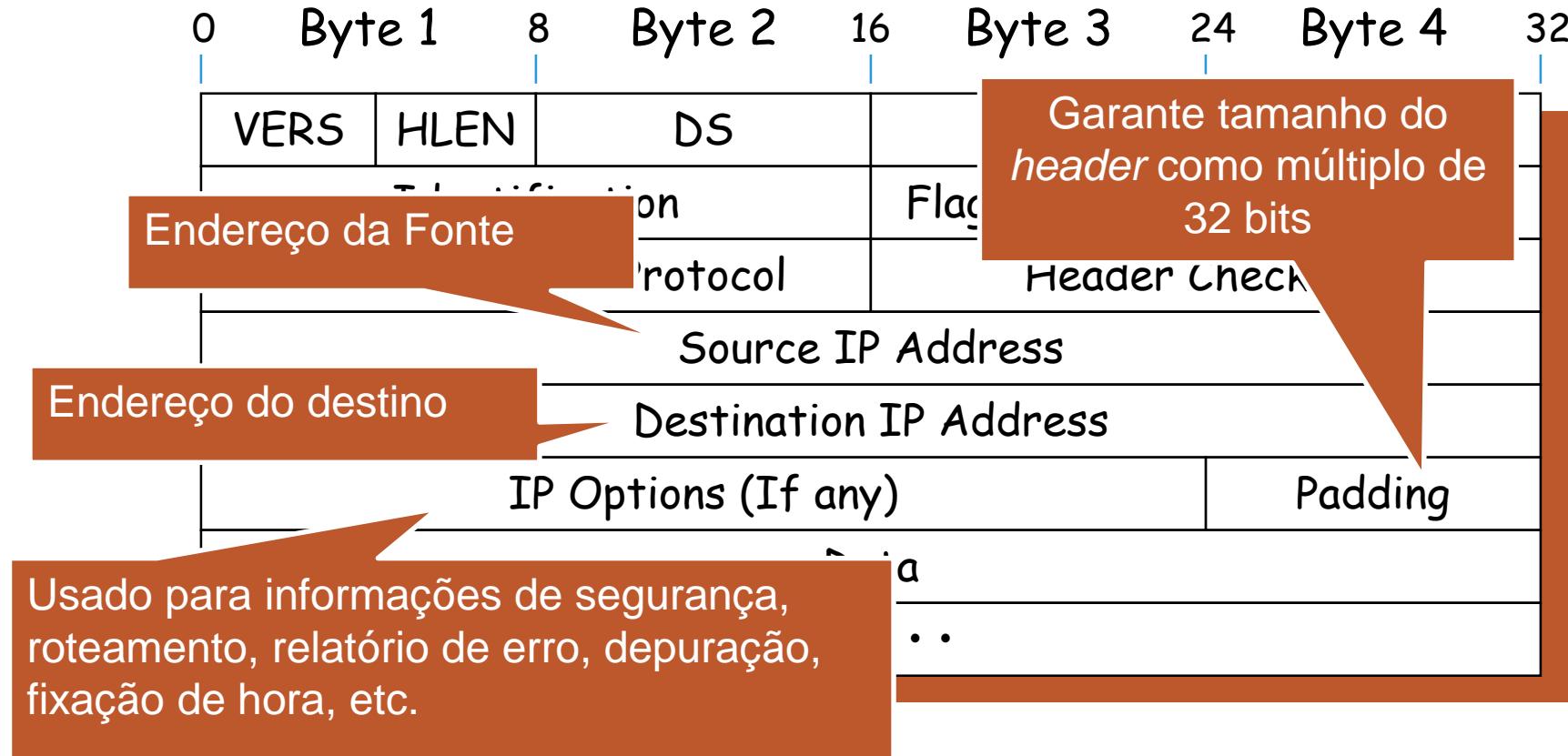
Usado para limitar o “tempo” de transmissão dos datagramas:

- Recebe um valor inicial
- Decrementado quando passa por um roteador
- Quando chega a zero datagrama é descartado

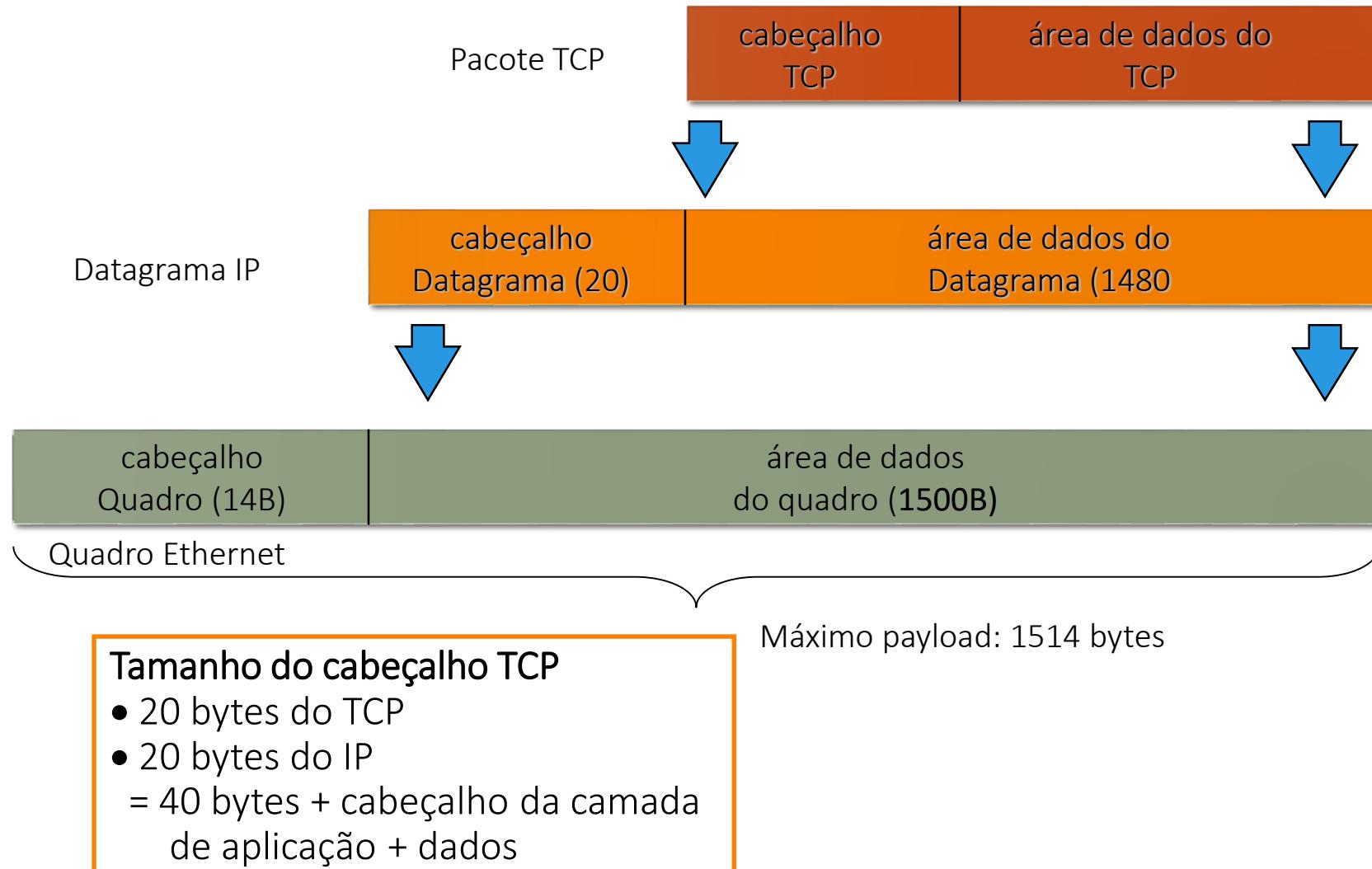


Formato do Datagrama IP

Formato do Datagrama IP



Encapsulamento de Datagramas



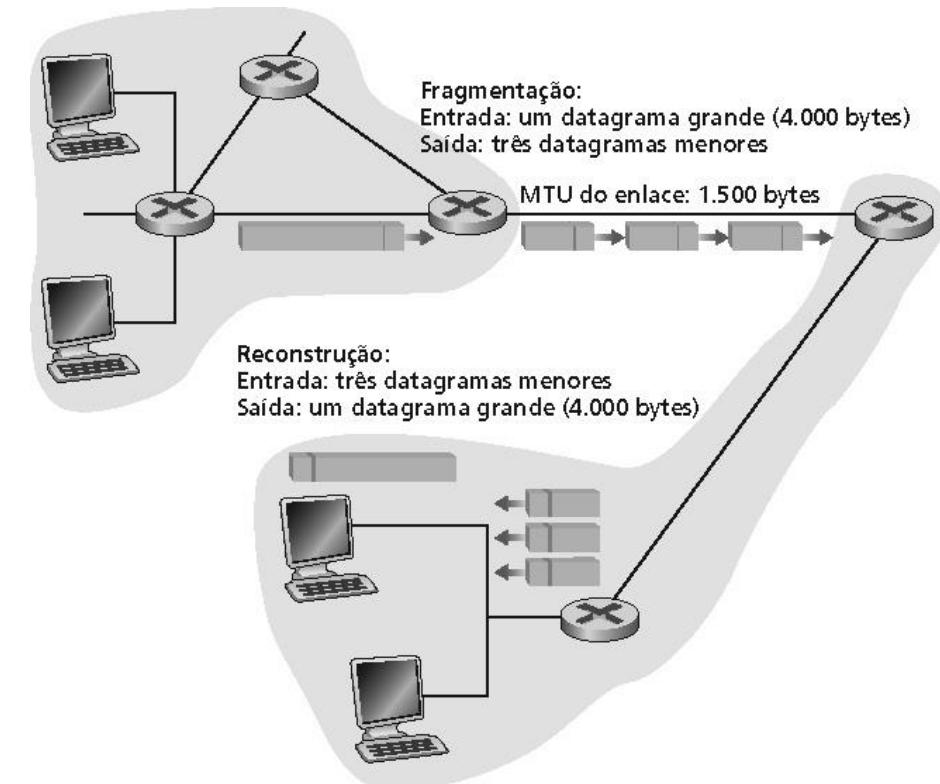
IP Fragmentação e Remontagem

Enlaces de rede têm MTU (max.transfer size)

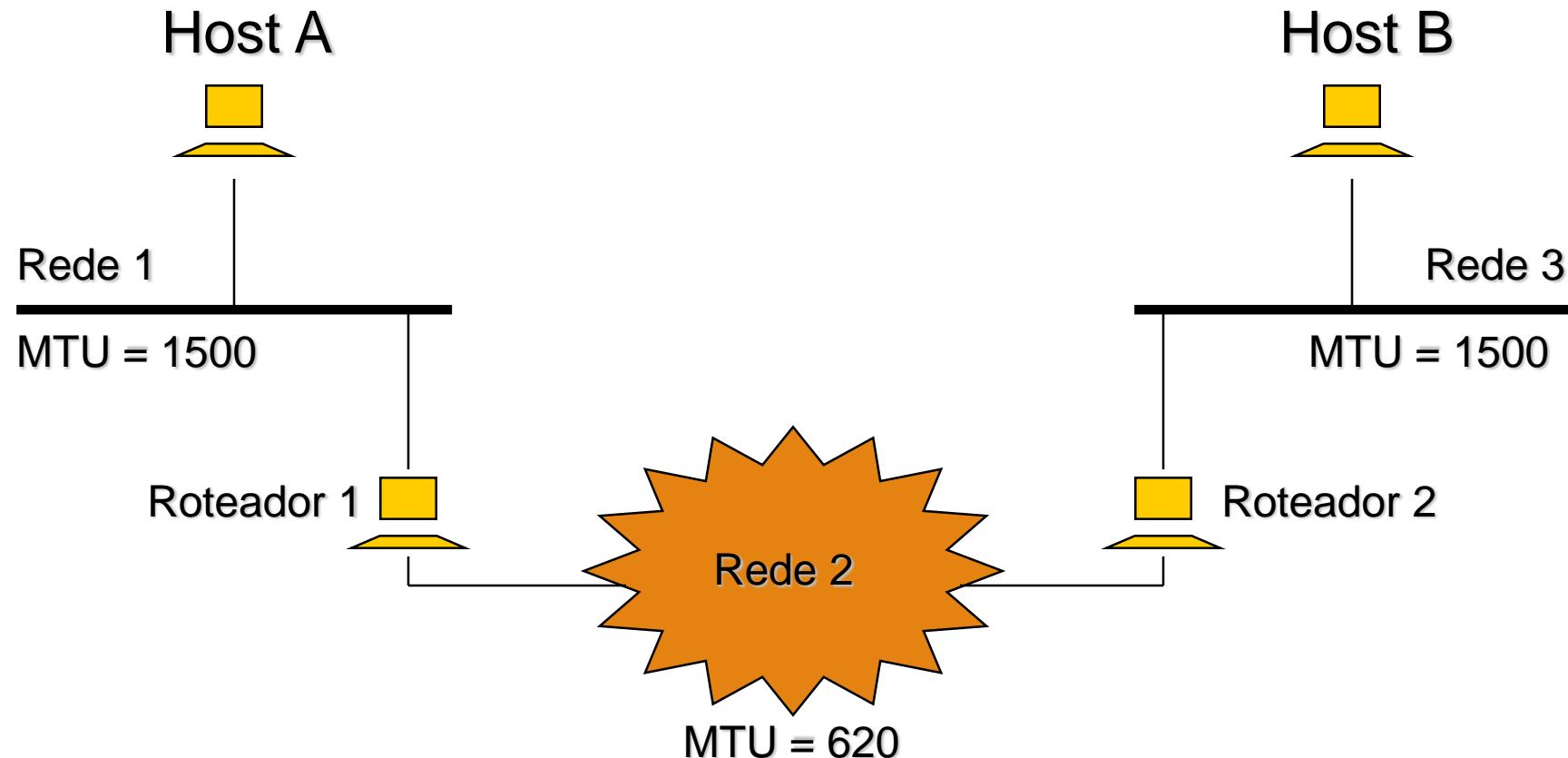
- corresponde ao maior frame que pode ser transportado pela camada de enlace.
- tipos de enlaces diferentes possuem MTU diferentes (ethernet: 1500 bytes)

Datagramas IP grandes devem ser divididos dentro da rede (fragmentados)

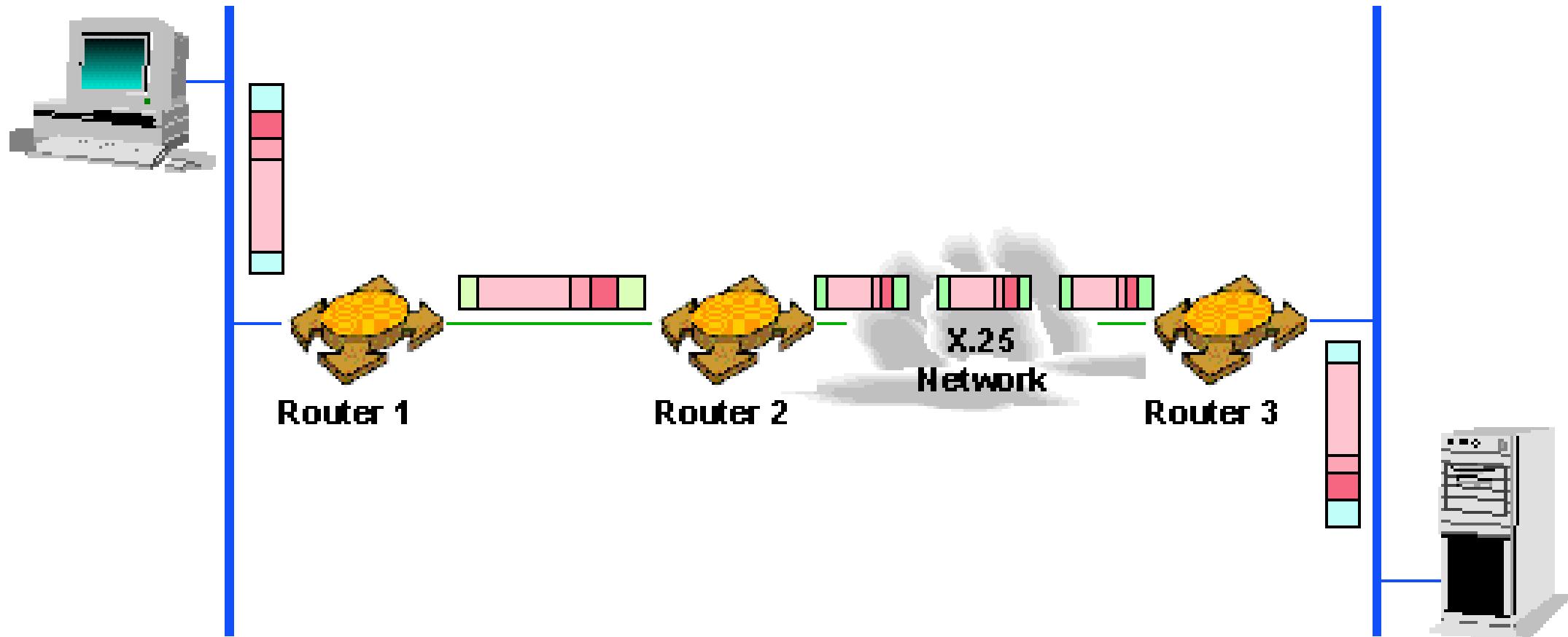
- um datagrama dá origem a vários datagramas
- “remontagem” ocorre apenas no destino final
- O cabeçalho IP é usado para identificar e ordenar datagramas relacionados



Fragmentação de Datagramas

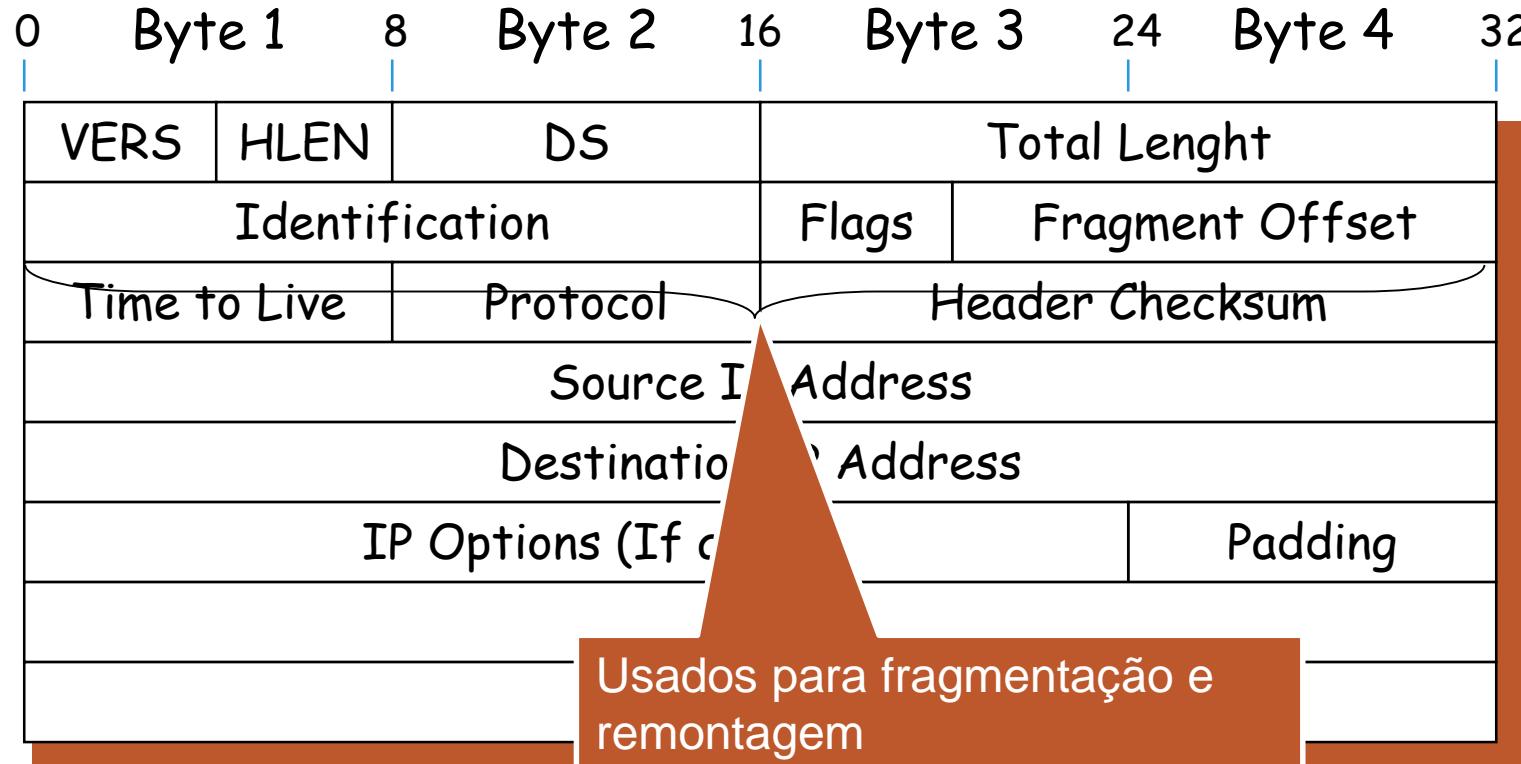


Fragmentação de Datagramas



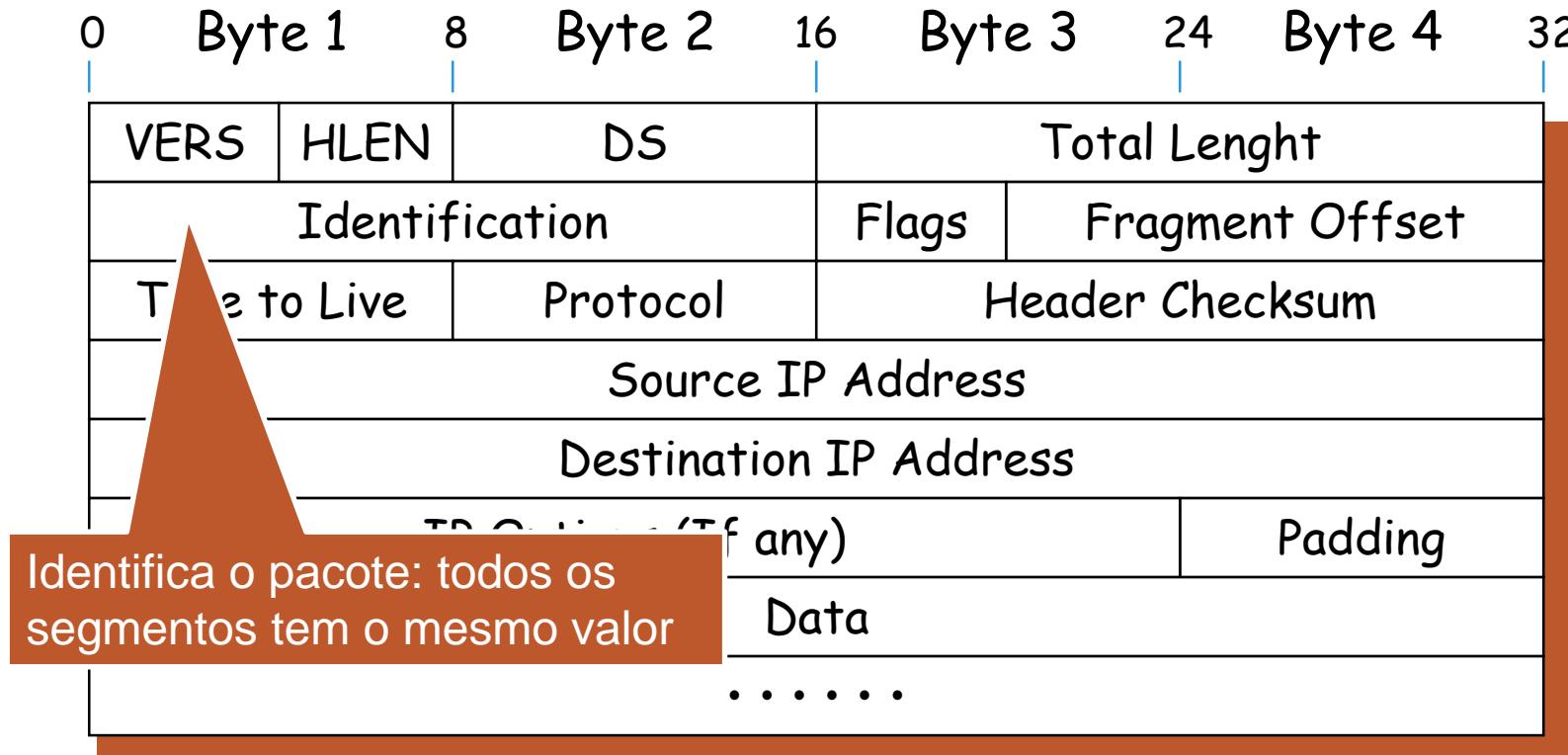
Formato do Datagrama IP

Formato do Datagrama IP



Formato do Datagrama IP

Formato do Datagrama IP



Fragmentação e Remontagem

Campo flags do cabeçalho IP (3 bits)

- 1 Bit reservado
- 1 Bit DF (don't fragment)
 - 1 indica que o pacote não pode ser fragmentado
 - Pois receptor não pode remontar
 - Roteadores tentam encontrar caminho sem fragmentação
 - Se não conseguir o pacote é descartado
- 1 Bit MF (more fragments)
 - 1 indica que existem mais fragmentos

IP Fragmentação e Remontagem

| | | | | | |
|--|------------------|----------|----------------|--------------|--|
| | tamanho =4000 | ID =x | fragflag =0 | offset =0 | |
|--|------------------|----------|----------------|--------------|--|

(4000-20=3980 bytes
de dados)

Um grande datagrama se torna
vários datagramas menores

| | | | | | |
|--|------------------|----------|----------------|--------------|--|
| | tamanho =1500 | ID =x | fragflag =1 | offset =0 | |
|--|------------------|----------|----------------|--------------|--|

(1500-20=1480
bytes de dados)

| | | | | | |
|--|------------------|----------|----------------|-----------------|--|
| | tamanho =1500 | ID =x | fragflag =1 | offset =1480 | |
|--|------------------|----------|----------------|-----------------|--|

(1500-20=1480
bytes de dados)

| | | | | | |
|--|------------------|----------|----------------|-----------------|--|
| | tamanho =1040 | ID =x | fragflag =0 | offset =2960 | |
|--|------------------|----------|----------------|-----------------|--|

(1040-20=1020
bytes de dados)

Fragmentação e Remontagem

Remontagem

- Módulo IP destinatário combina os datagramas IP que possuem o mesmo valor para os campos identification, protocol, source address e destination address
- Feita através da colocação da porção de dados de cada fragmento na posição relativa indicada pelo valor de fragment-offset
 - Primeiro fragmento possui o fragment-offset igual a 0
 - Último fragmento tem um flag more fragments igual a 0

Pontos Importantes

Protocolo IP

- Entender os serviços oferecidos pelo protocolo

CAP 6. CAMADA DE REDE

AULA 6: ICMP E TRACEROUTE

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

ICMP: Internet Control Message Protocol

Usado por hosts, routers, para comunicações a nível de rede

- Relato de erros: protocolo, porta, rede, host não encontrado
- echo request/reply (usado pelo ping)

Msgs ICMP

- são transportados em pacotes IP

Mensagens ICMP: type, code mais primeiros 8 bytes do datagrama IP causando erro

| Type | Code | description |
|------|------|---|
| 0 | 0 | echo reply (ping) |
| 3 | 0 | dest. network unreachable |
| 3 | 1 | dest host unreachable |
| 3 | 2 | dest protocol unreachable |
| 3 | 3 | dest port unreachable |
| 3 | 6 | dest network unknown |
| 3 | 7 | dest host unknown |
| 4 | 0 | source quench (congestion control - not used) |
| 8 | 0 | echo request (ping) |
| 9 | 0 | route advertisement |
| 10 | 0 | router discovery |
| 11 | 0 | TTL expired |
| 12 | 0 | bad IP header |

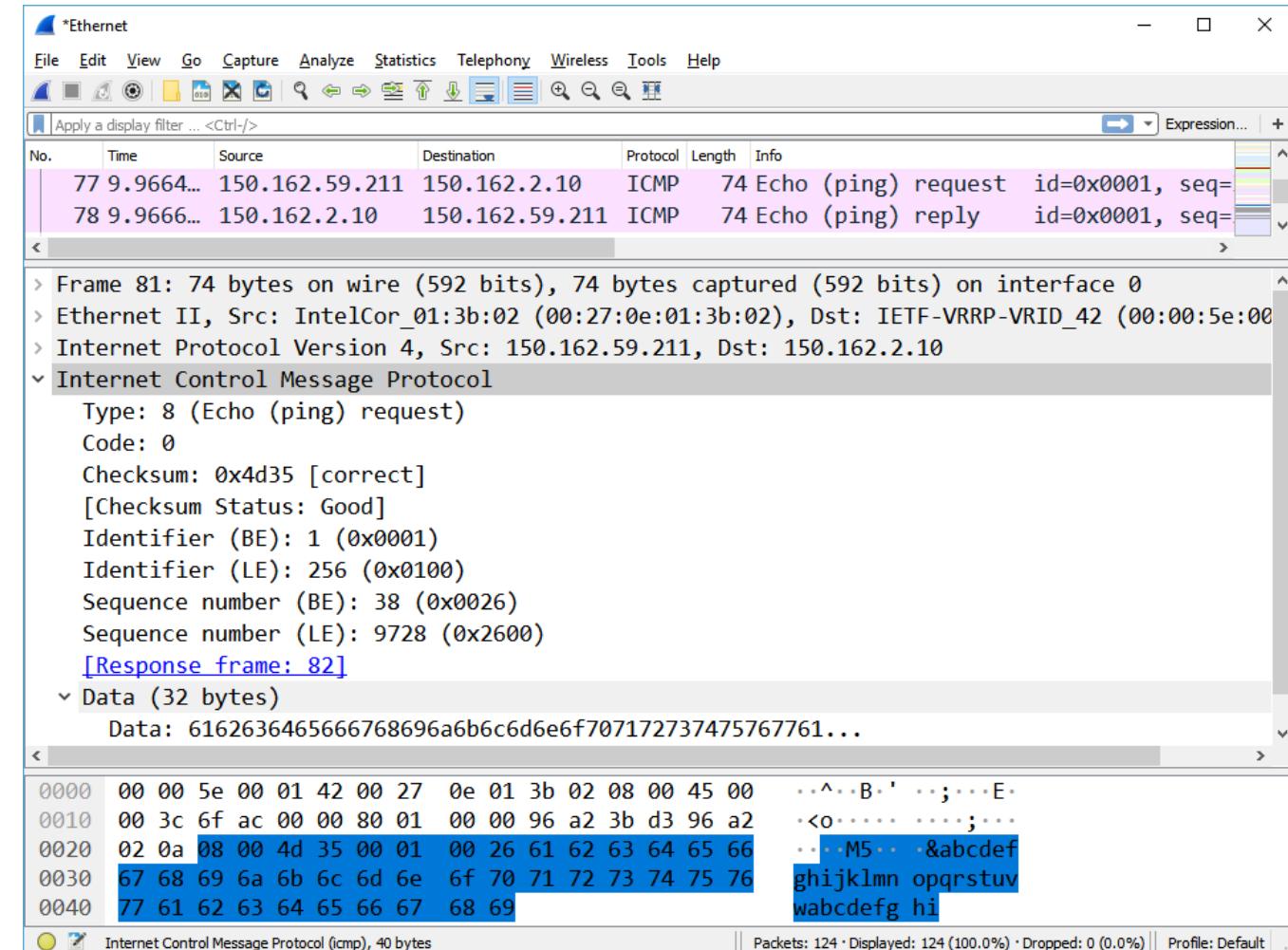
ICMP: Internet Control Message Protocol

Msgs ICMP

- são transportados em pacotes IP

Mensagens ICMP:

- type, code mais primeiros 8 bytes do datagrama IP causando erro



Traceroute e ICMP

O transmissor envia uma série de segmentos UDP para o destino
(ICMP Echo Request)

- 1º possui TTL = 1, 2º possui TTL = 2 ... Incrementa TTL em cada tentativa até encontrar o destino

Quando o enésimo datagrama chega ao enésimo roteador:

- O roteador descarta o datagrama
- E envia à origem uma mensagem ICMP (type 11, code 0)
- A mensagem inclui o nome do roteador e o endereço IP

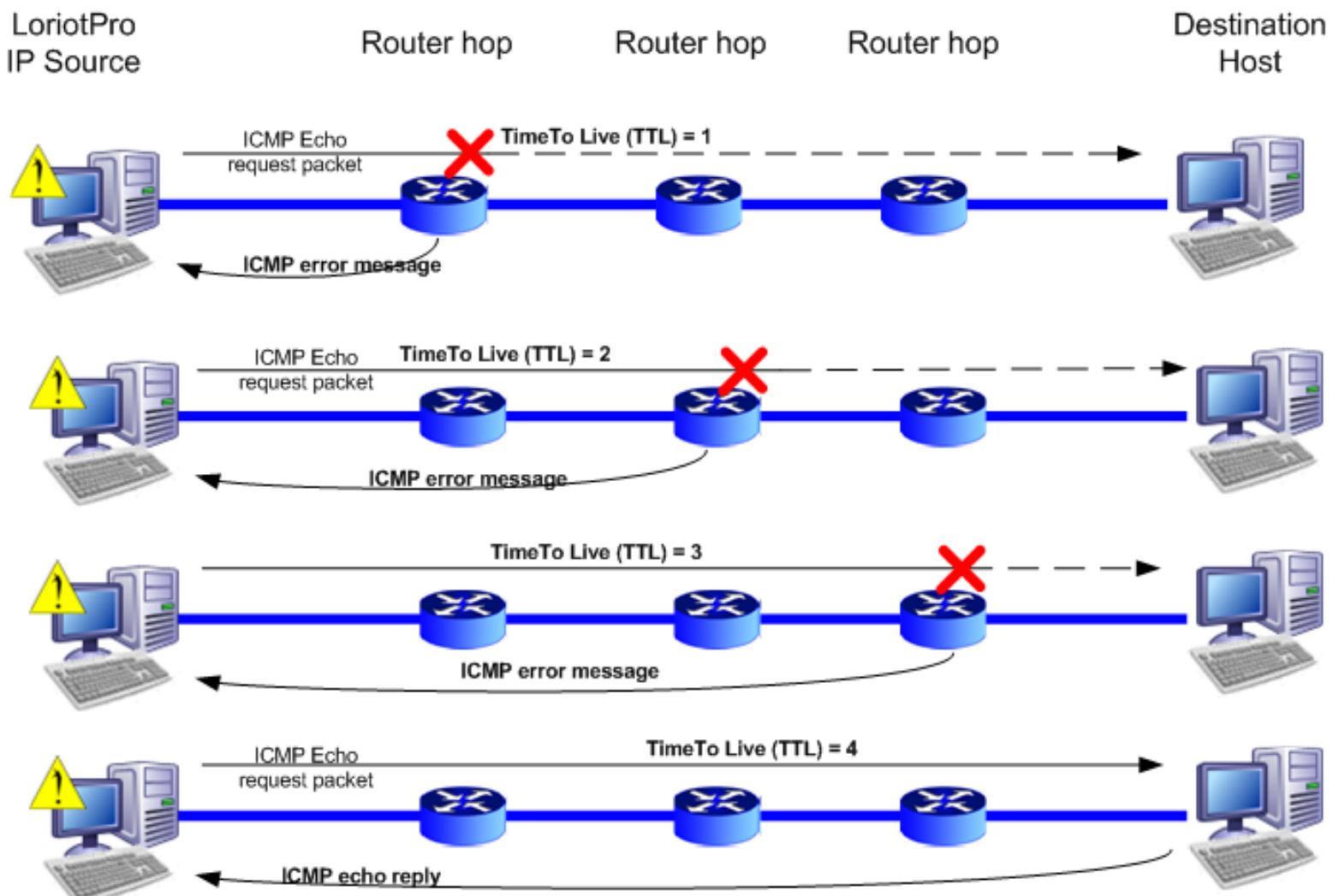
Quando a mensagem ICMP chega, a origem calcula o RTT

- O traceroute faz isso três vezes

Critério de interrupção

- O segmento UDP finalmente chega ao hospedeiro de destino
- O destino retorna o pacote ICMP “Echo Reply” (type 0, code 0)

Traceroute e ICMP



Traceroute e ICMP

```
Windows Prompt de Comando  
C:\Users\willrich>tracert www.ietf.org  
Rastreando a rota para www.ietf.org [12.22.58.30]  
com no máximo 30 saltos:  
  
 1   16 ms      6 ms      *       150.162.239.253  
 2   29 ms      25 ms     16 ms   popsc-10g-ufsc-te-1-2-rt1.bb.pop-sc.rnp.br [200.  
237.194.45]  
 3   30 ms      71 ms      9 ms   xe-2-0-0-2910-r0-sc.bkb.rnp.br [200.143.254.161]  
 4   374 ms     183 ms    117 ms   xe-3-1-1-3000-r0-sp.bkb.rnp.br [200.143.252.65]  
 5   158 ms     173 ms    179 ms   200.143.254.234  
 6   133 ms     134 ms    177 ms   66.165.175.25  
 7   *          168 ms      *       t0-0-0-5.br2.mia.terremark.net [66.165.161.93]  
 8   *          213 ms    161 ms   12.88.168.13  
 9   210 ms      *          *       cr1.ormfl.ip.att.net [12.122.143.50]  
10   247 ms      *          218 ms   cr2.hsitx.ip.att.net [12.122.1.5]  
11   218 ms      *          *       cr1.dltx.ip.att.net [12.122.28.157]  
12   203 ms     206 ms    218 ms   cr2.dltx.ip.att.net [12.122.1.210]  
13   249 ms     223 ms    215 ms   cr2.la2ca.ip.att.net [12.122.28.178]  
14   205 ms     206 ms    225 ms   cr1.la2ca.ip.att.net [12.122.2.165]  
15   305 ms      *          230 ms   cr82.sj2ca.ip.att.net [12.122.1.146]  
16   243 ms     256 ms      *       gar14.sffca.ip.att.net [12.122.110.9]  
17   *          205 ms    214 ms   12.94.198.6  
18   205 ms     232 ms    220 ms   mail.ietf.org [12.22.58.30]  
  
Rastreamento concluído.  
C:\Users\willrich>
```

Pontos Importantes

Protocolo ICMP e Traceroute

- Entender os objetivos do protocolo ICMP
- Conhecer o funcionamento do traceroute

CAP 6. CAMADA DE REDE

AULA 7: ARQUITETURA DE UM ROTEADOR

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

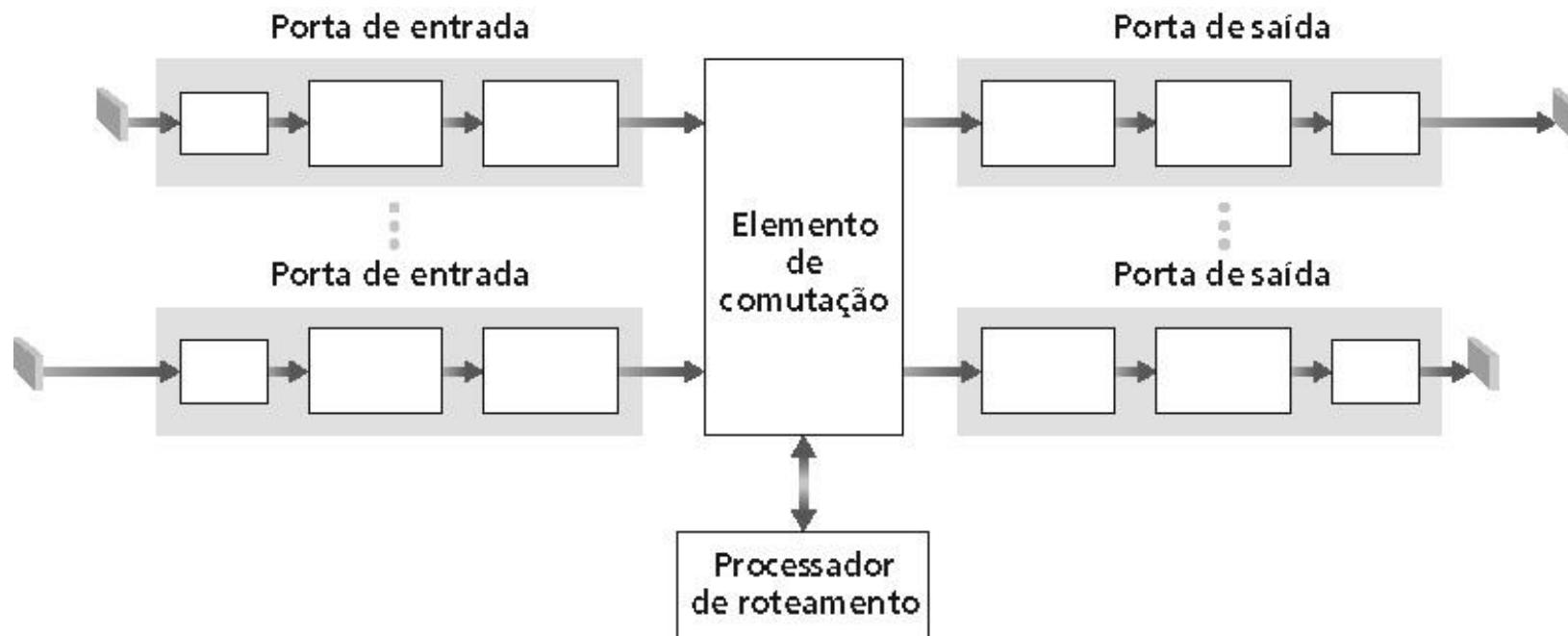
ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

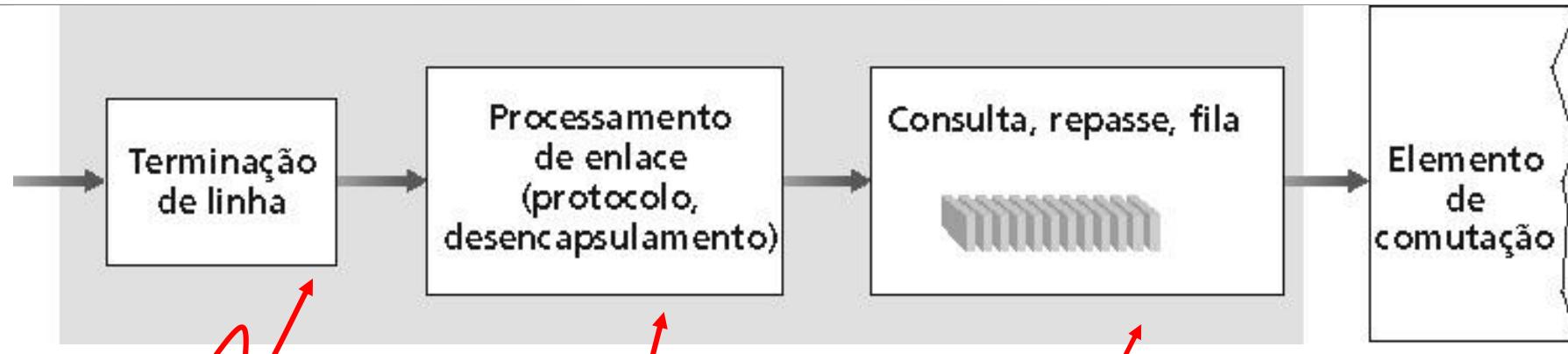
Arquitetura de um Roteador

Duas funções chaves do roteador:

- Executar algoritmos/protocolos de roteamento (RIP, OSPF, BGP)
- Comutar datagramas de enlaces de entrada para enlaces de saída



Funções da porta de entrada



Camada Física:

Recepção a nível de bit

Camada de Enlace:
(ex.:Ethernet)

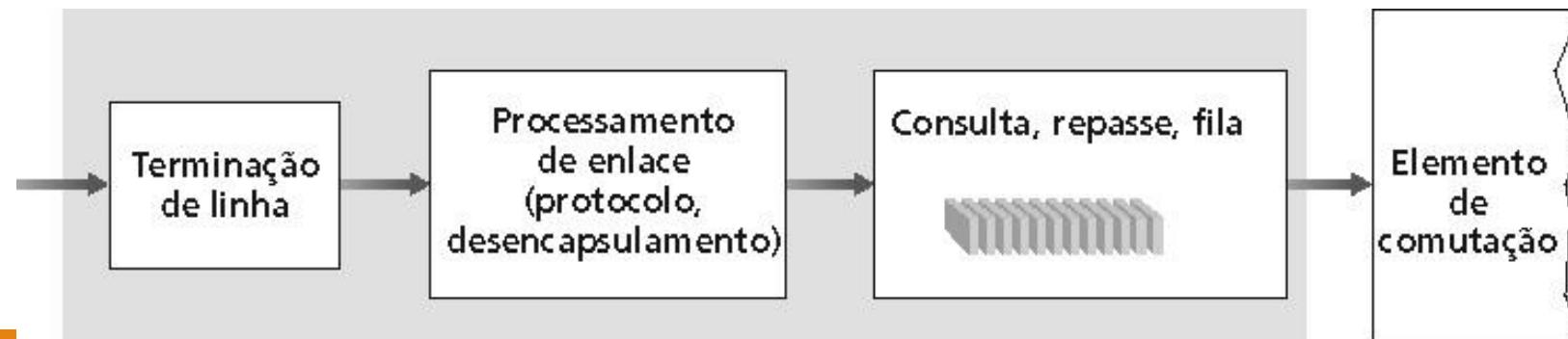
Comutação descentralizada:

- Dado o destino do datagrama, procura a porta de saída usando a tabela de roteamento na memória da porta de entrada
- Objetivo: completar o processamento da porta de entrada na 'velocidade do enlace'
- Fila: se os datagramas chegam mais rápido do que a taxa de comutação do elemento de comutação

Funções da porta de entrada

Funções da fila de entrada

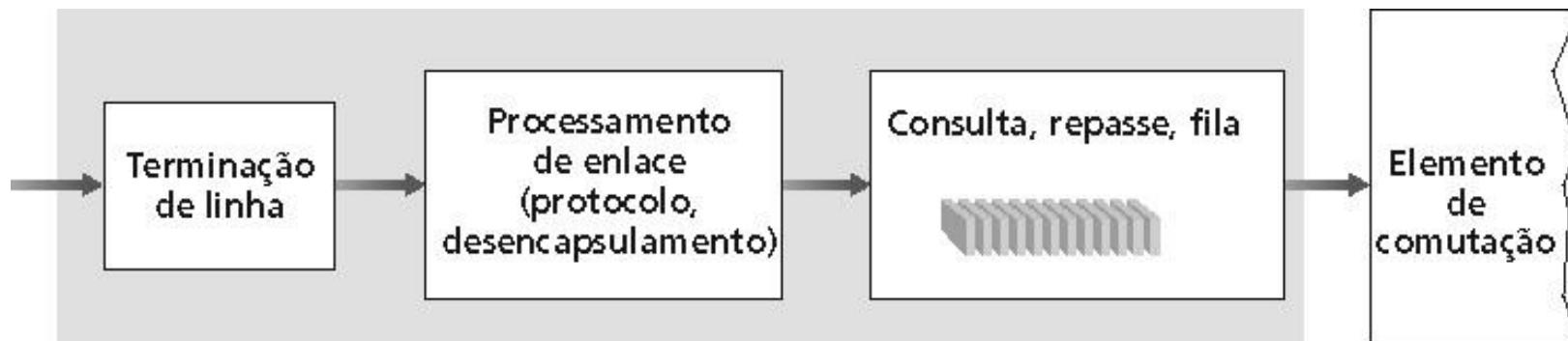
- Consulta tabela de roteamento e encaminha pacote para porta de saída
 - Escolha da porta de saída é feita usando a tabela de roteamento
 - Tabela de roteamento é computada pelo processador de roteamento e cada porta de entrada mantém uma cópia
 - Com cópias locais a decisão de comutação pode ser feita localmente sem invocar o processador centralizado
 - Tal comutação descentralizada evita a ocorrência de um gargalo de processamento em um único ponto



Funções da porta de entrada

Em roteadores com capacidades de processamento limitadas

- A porta de entrada pode simplesmente encaminhar o pacote para o processador de roteamento central
- Processador central consulta a tabela e encaminha pacote para a porta de saída apropriada
- Abordagem realizada quando uma estação de trabalho ou servidor atua como roteador
 - Processador de roteamento é a própria CPU da máquina
 - Porta de entrada é a placa de interface de rede



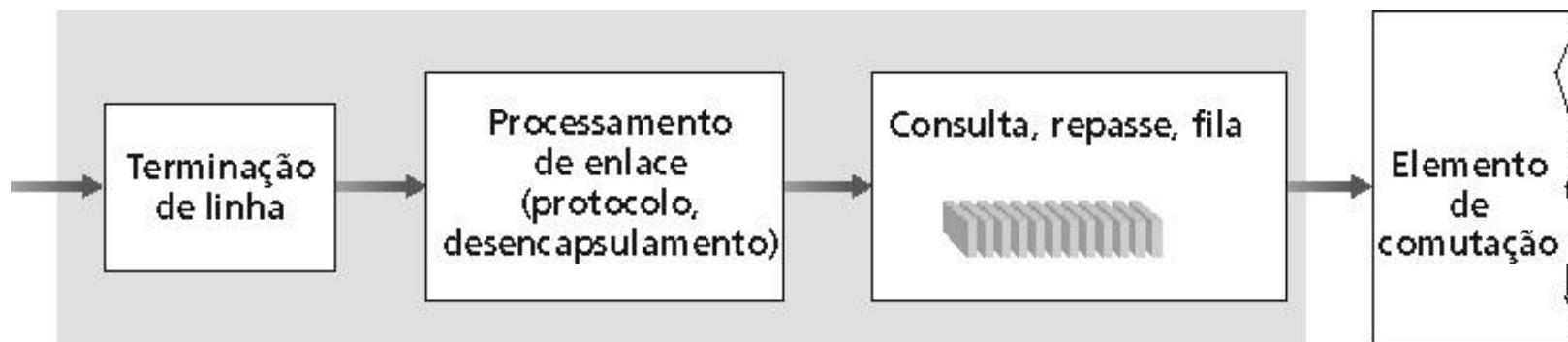
Funções da porta de entrada

Uma vez determinada a porta de saída apropriada

- O pacote pode ser encaminhado via o elemento de comutação
- Mas pacote pode ter a entrada temporariamente bloqueada
 - Se o elemento de comutação estiver ocupada enviando outro pacote
- Pacotes bloqueado são colocados em uma fila na porta de entrada

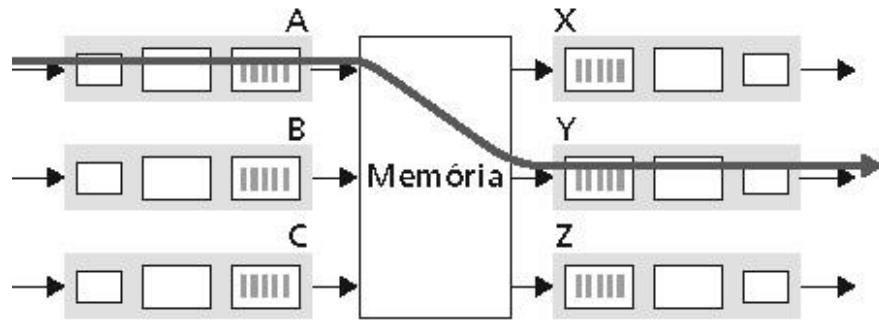
Pacotes de controle (RIP, OSPF ou BGP)

- São encaminhados para o processador de roteamento

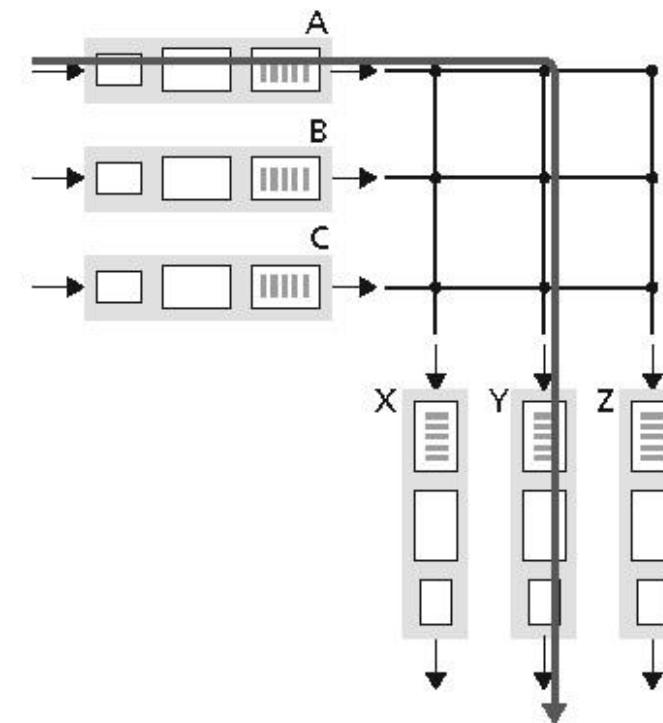


Três tipos de Elementos de Comutação

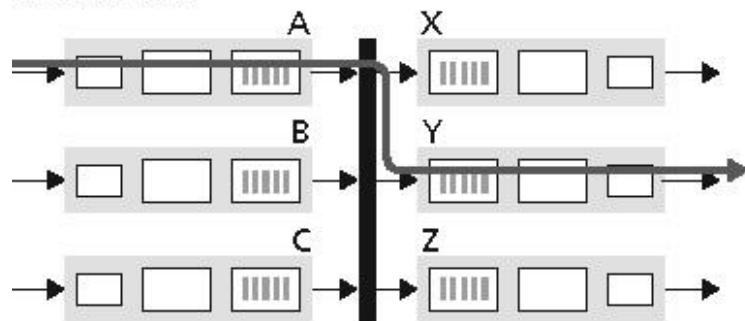
Memória



Crossbar



Barramento



Legenda:



Porta de entrada



Porta de saída

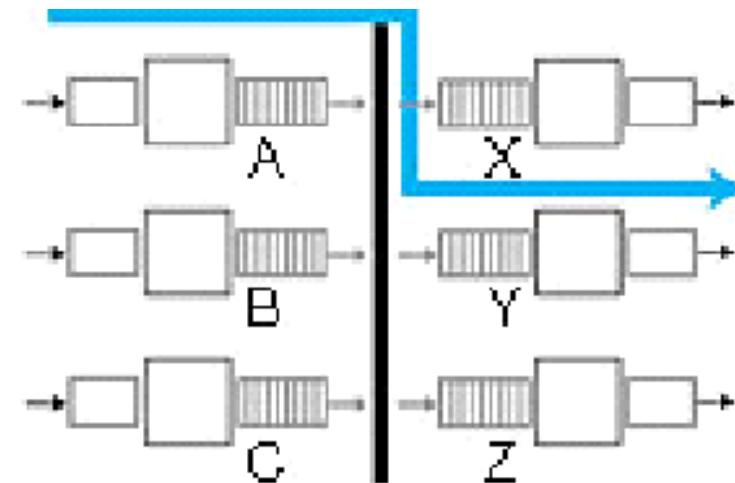
Comutação Via Barramento

Comutação

- Datagrama é encaminhado da memória da porta de entrada para a memória da porta de saída via barramento compartilhado

Contenção no barramento

- Velocidade de comutação limitada pela velocidade do barramento
- Barramento de 1 Gbps é suficiente para roteadores de acesso e de empresas (Não para regional ou backbones)
- Cisco 1900 é de 1 Gbps
- 3Com CoreBuilder 5000 systems é de 2 Gbps



Comutação Cross-bar (rede ou matriz de interconexão)

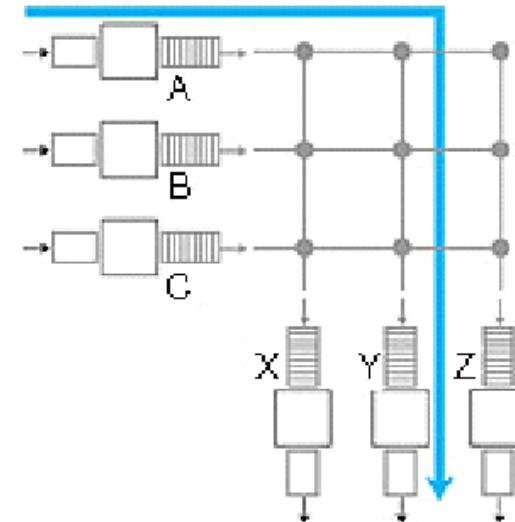
Supera as limitações de largura de banda do barramento

Redes de Banyan

- interconexão inicialmente desenvolvidas para conectar processadores em multiprocessamento

Portas interconectadas

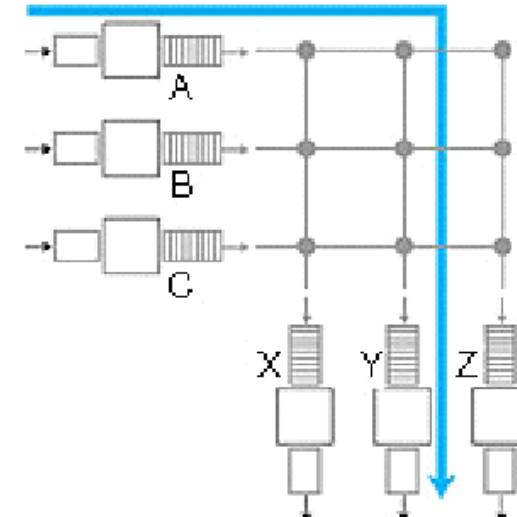
- $2N$ barramentos que conectam N portas de entrada a N portas de saída
- Portas podem se comunicar ao mesmo tempo (com paralelismo)



Comutação Cross-bar (rede ou matriz de interconexão)

Comutação

- Pacote que chega na porta de entrada atravessa o barramento horizontal ligado a porta de entrada até a intersecção com o barramento vertical levando a porta de saída
- Se o barramento vertical é livre o pacote é transmitido para a porta de saída
- Se ocupado o pacote é bloqueado e deve ser enfileirado na porta de entrada

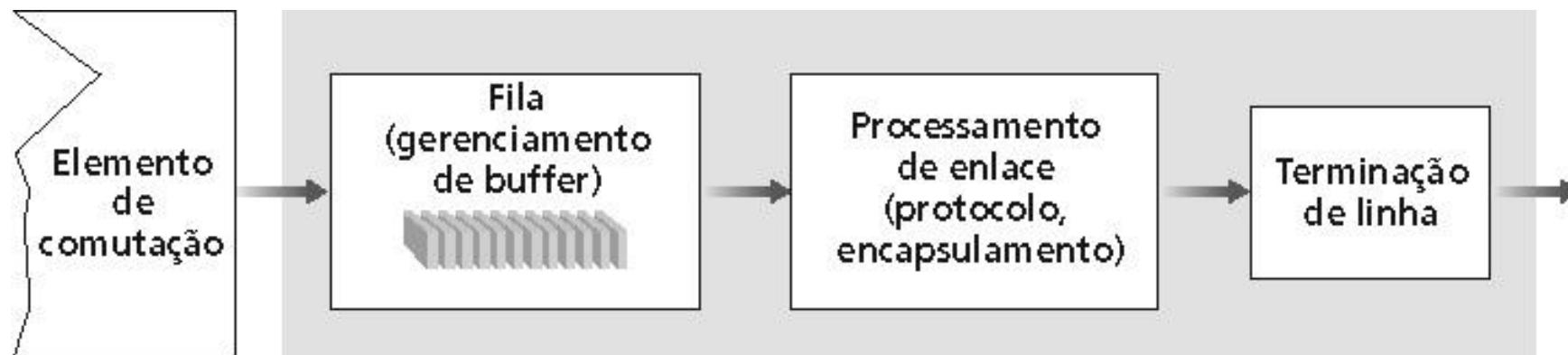


Portas de Saída

Bufferização é necessária quando datagramas chegam do elemento de comutação mais rápido que a taxa de transmissão

- Enfileiramento (atraso) e perda devido ao overflow de buffers de saída

Disciplinas de escalonamento escolhem entre datagramas na fila para transmissão



Pontos Importantes

Arquitetura de um roteador

- Entender o funcionamento de um roteador

CAP 6. CAMADA DE REDE

AULA 8: ROTEAMENTO

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

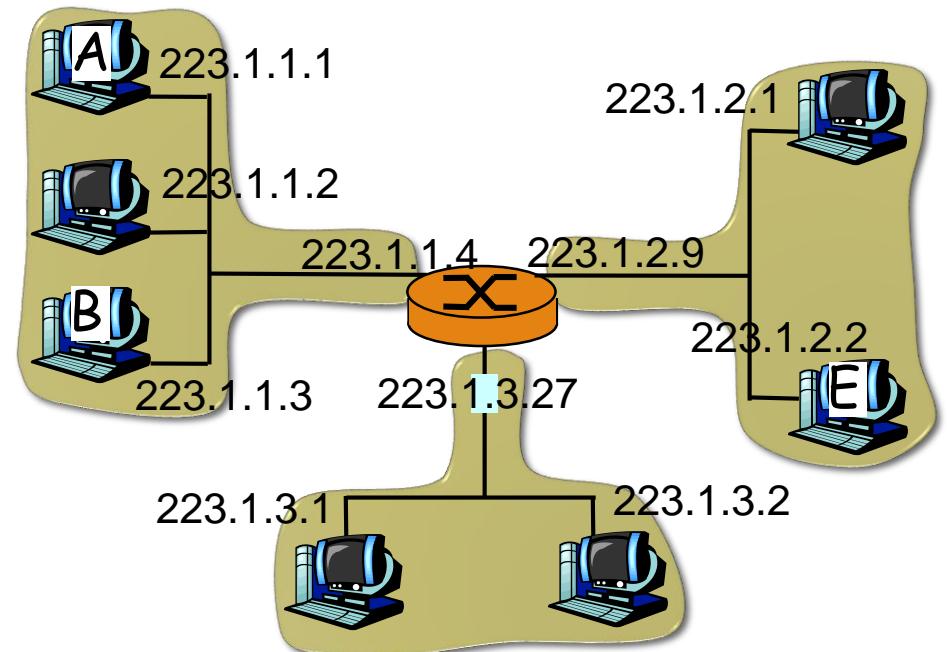
ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

Roteamento

Roteamento inter-redes é a principal função do protocolo IP

- Protocolo IP assume que um host sabe enviar datagramas para qualquer host da mesma rede local
- Roteador entra em ação no momento que um datagrama tem destino fora da rede local
- Host origem envia o datagrama para o gateway (roteador)

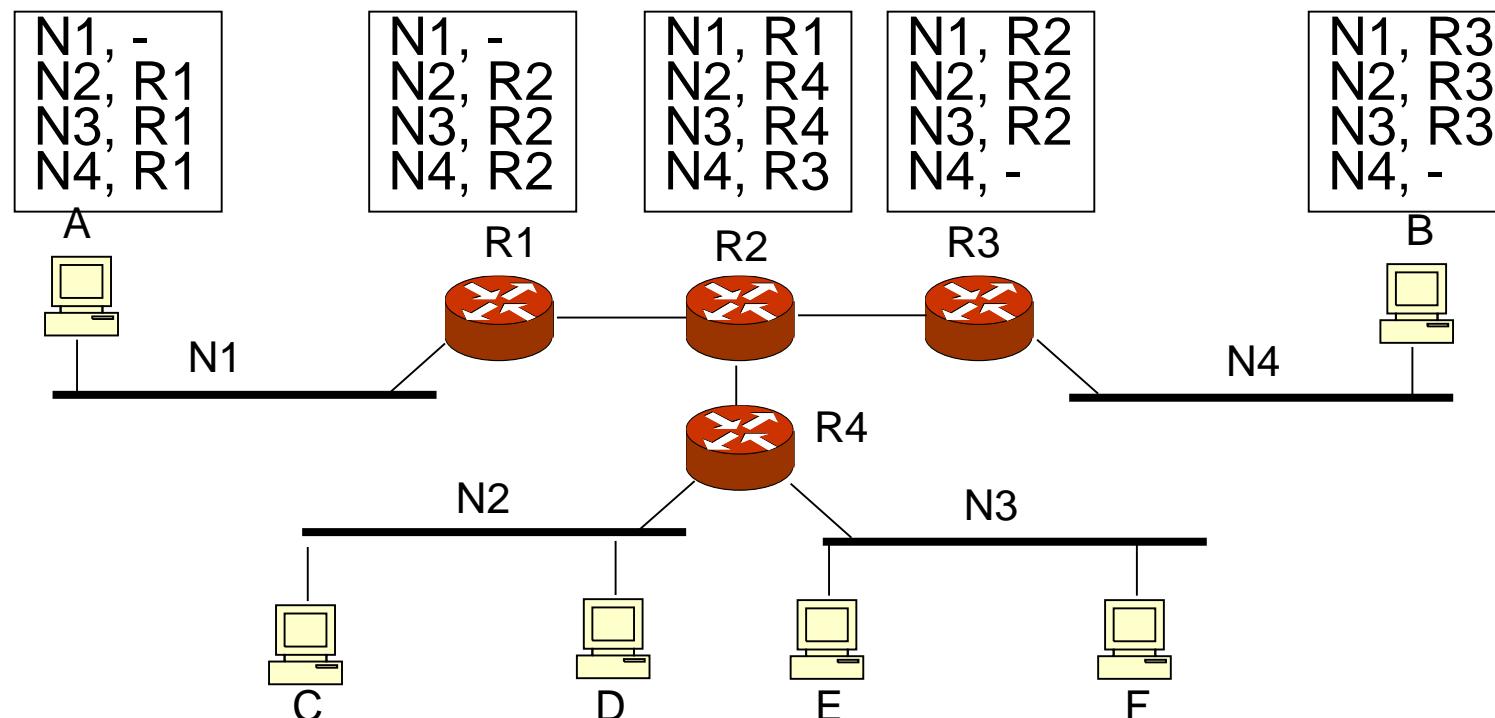


Roteamento e Tabelas de Roteamento

Como manter informações sobre rotas de A para qualquer outro host?

- A → R1 → R2 → R3 → B

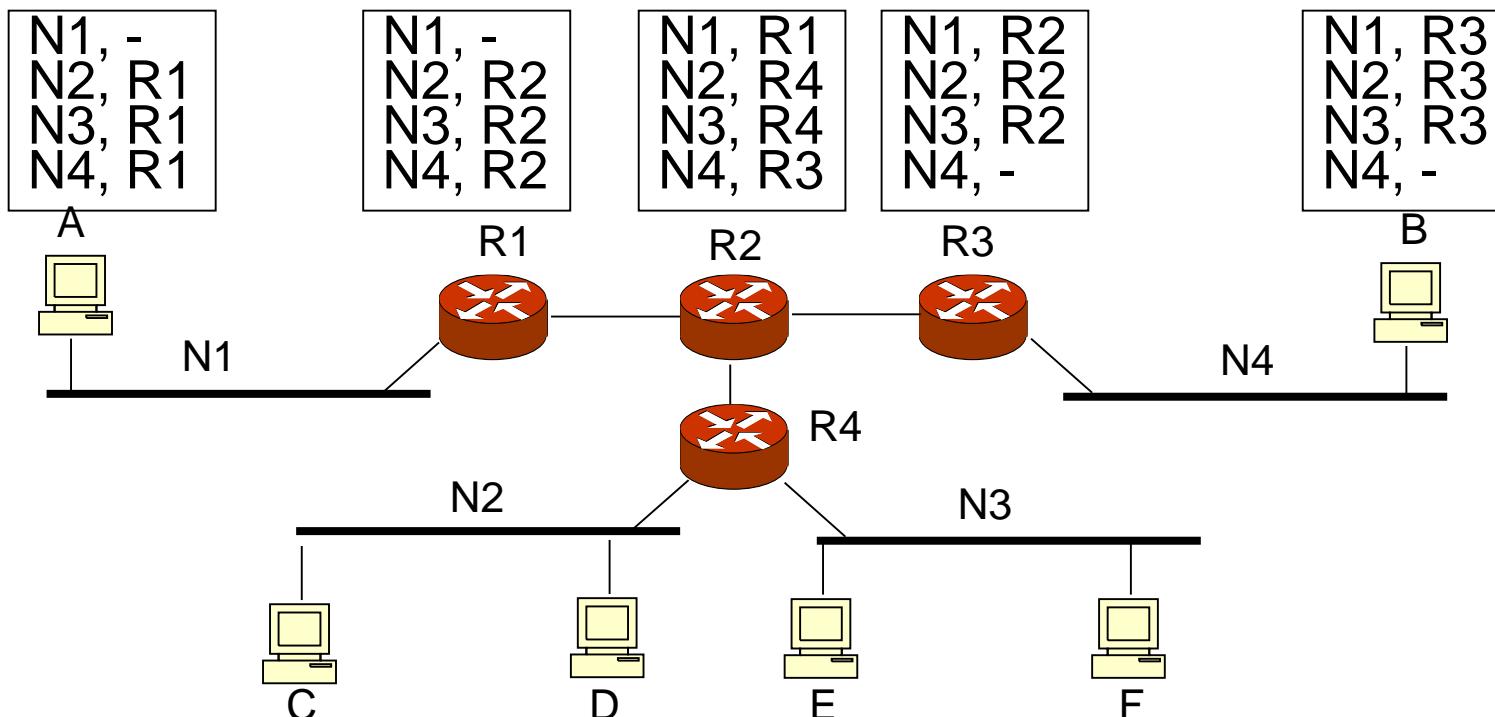
Cada nó armazena endereço de rede e próximo hop



Tipos de Roteamento

Estático

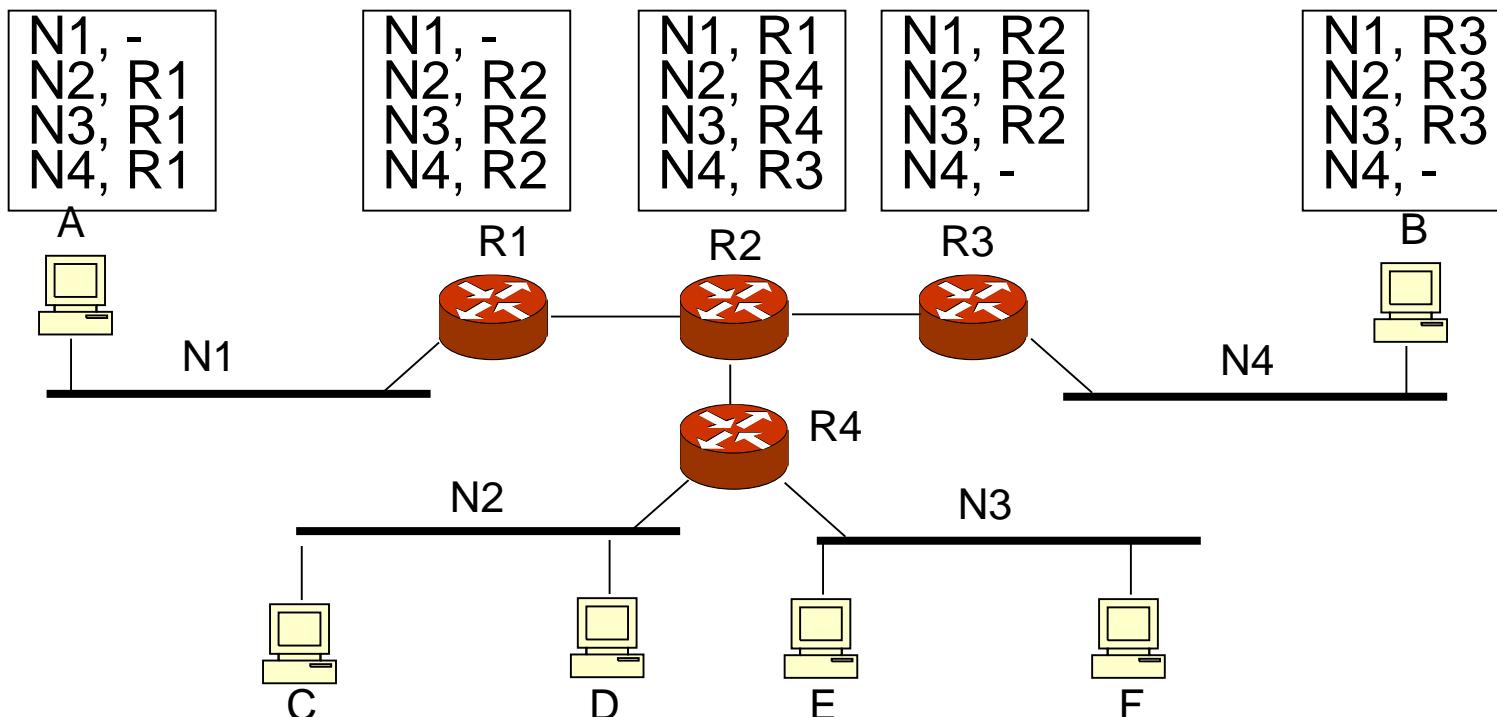
- Configurado pelo administrador no roteador
- Não se adapta a mudanças na topologia da rede
- Informação não é trocada com outros roteadores, por default (+ segurança)



Tipos de Roteamento

Dinâmico

- Administrador configura parâmetros iniciais
- Protocolos de roteamento são usados para trocar informações entre roteadores
- Adaptação automática em caso de mudança de topologia



Protocolos de Roteamento

Objetivos

- Gerenciar a tabela de roteamento dinamicamente, com rota para “todas” as redes
- Se há mais de uma rota para uma rede, a com o menor custo é colocada na tabela de roteamento
- Adicionar novas rotas, trocar por melhores naquele momento
- Prevenir loops de roteamento

Roteamento IP

Estratégia de roteamento:

- Se host destino está na mesma rede => envia datagrama diretamente (endereço MAC)
 - Verifica pelo End. IP de destino e máscara
- Senão => envia a um gateway local (endereço MAC)

Levando um Datagrama da Fonte ao Destino

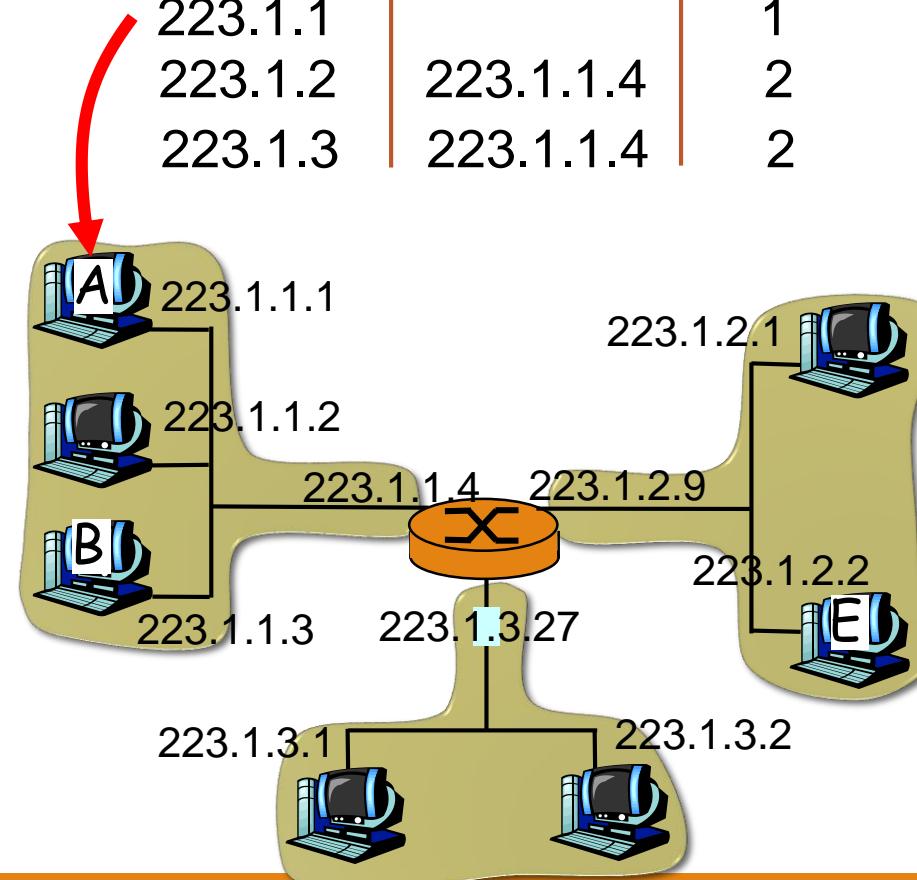
Datagrama IP:

| | | | |
|---------------|--------------------|---------------------|-------|
| outros campos | endereço IP origem | endereço IP destino | dados |
|---------------|--------------------|---------------------|-------|

- os endereços do datagrama não mudam ao viajar da fonte ao destino

tabela de roteamento em A

| Rede destino | próx. roteador | Nºm. saltos |
|--------------|----------------|-------------|
| 223.1.1 | | 1 |
| 223.1.2 | 223.1.1.4 | 2 |
| 223.1.3 | 223.1.1.4 | 2 |



Roteamento IP

Comando “route print” no host 192.168.0.194

```
cmd Prompt de Comando
C:\Users\willrich>route print -4
=====
Lista de interfaces
14...00 1c bf 1c 53 7b ....Intel(R) PRO/Wireless 3945ABG Network Connection
11...00 1b 24 95 70 bf ....Broadcom NetLink(TM) Gigabit Ethernet
1.....00 00 00 00 00 00 Software Loopback Interface 1
15...00 00 00 00 00 e0 Microsoft 6to4 Adapter #2
12...00 00 00 00 00 e0 Microsoft 6to4 Adapter
13...00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
17...00 00 00 00 00 e0 Microsoft 6to4 Adapter #3
16...00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
26...00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

Tabela de rotas IPv4
=====
Rotas ativas:
Endereço de rede      Máscara    Ender. gateway      Interface   Custo
          0.0.0.0        0.0.0.0      192.168.0.1      192.168.0.194    25
          127.0.0.0       255.0.0.0     No vínculo        127.0.0.1     306
          127.0.0.1       255.255.255.255  No vínculo        127.0.0.1     306
         127.255.255.255 255.255.255.255  No vínculo        127.0.0.1     306
          192.168.0.0       255.255.255.0     No vínculo      192.168.0.194    281
          192.168.0.194     255.255.255.255  No vínculo      192.168.0.194    281
          192.168.0.255     255.255.255.255  No vínculo      192.168.0.194    281
          224.0.0.0         240.0.0.0     No vínculo        127.0.0.1     306
          224.0.0.0         240.0.0.0     No vínculo      192.168.0.194    281
         255.255.255.255 255.255.255.255  No vínculo        127.0.0.1     306
         255.255.255.255 255.255.255.255  No vínculo      192.168.0.194    281
=====
Rotas persistentes:
Nenhuma
C:\Users\willrich>
```

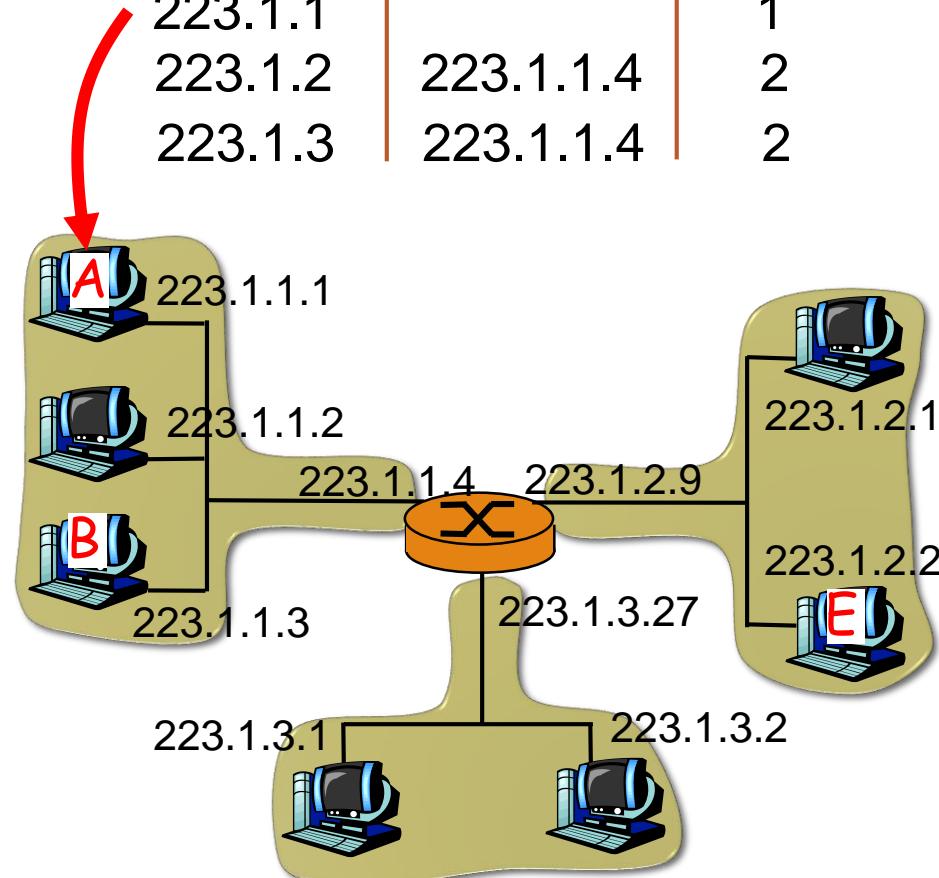
Levando um Datagrama da Fonte ao Destino

| | | | |
|---------------|-----------|-----------|-------|
| outros campos | 223.1.1.1 | 223.1.1.3 | dados |
|---------------|-----------|-----------|-------|

A envia datagrama IP para B:

- examina endereço de rede de B
- descobre que B está na mesma rede de A
- camada de enlace envia datagrama diretamente para B num quadro da camada de enlace
- Se necessário descobre endereço físico de B (usando ARP)

| Rede destino | Próx. roteador | Núm. saltos |
|--------------|----------------|-------------|
| 223.1.1 | | 1 |
| 223.1.2 | 223.1.1.4 | 2 |
| 223.1.3 | 223.1.1.4 | 2 |



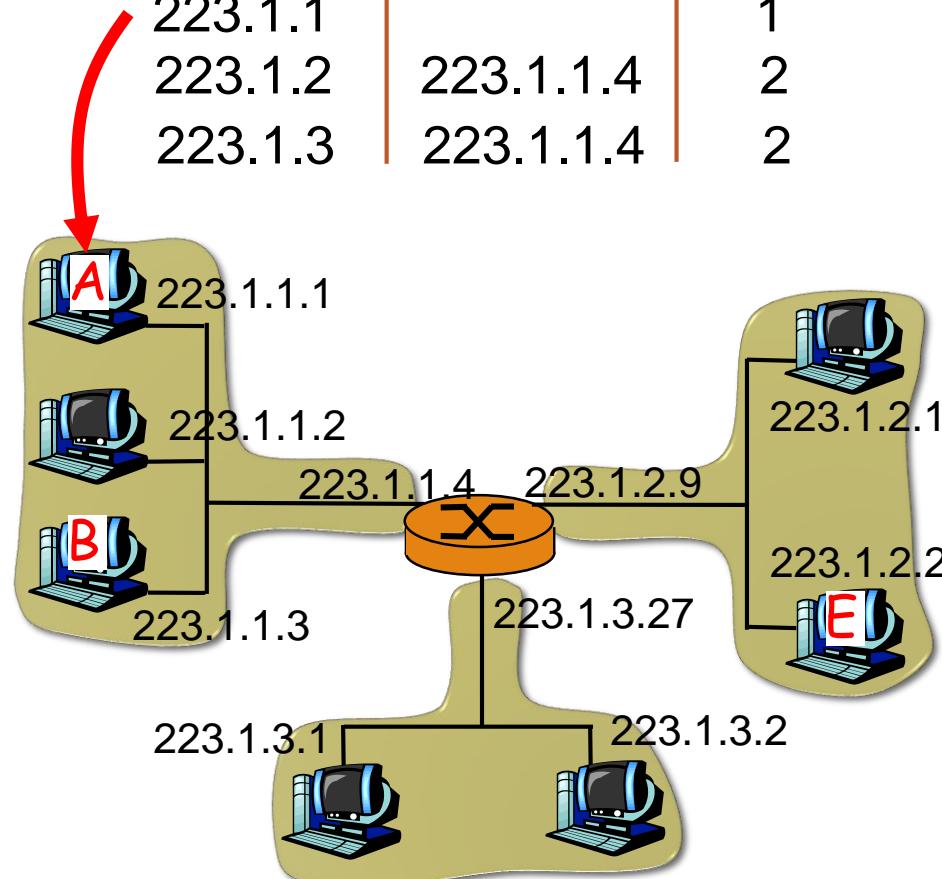
Levando um Datagrama da Fonte ao Destino

| | | | |
|---------------|-----------|-----------|-------|
| outros campos | 223.1.1.1 | 223.1.2.2 | dados |
|---------------|-----------|-----------|-------|

A envia datagrama IP para E:

- examina endereço de rede de E
- E está numa rede diferente
 - A, E não estão diretamente conectados
- tabela de roteamento: próximo roteador para E é 223.1.1.4
- encontra endereço físico de 223.1.1.4 e envia o datagrama num quadro de enlace
- datagrama chega em 223.1.1.4
- continua.....

| Rede destino | Próx. roteador | Nºm. saltos |
|--------------|----------------|-------------|
| 223.1.1 | | 1 |
| 223.1.2 | 223.1.1.4 | 2 |
| 223.1.3 | 223.1.1.4 | 2 |



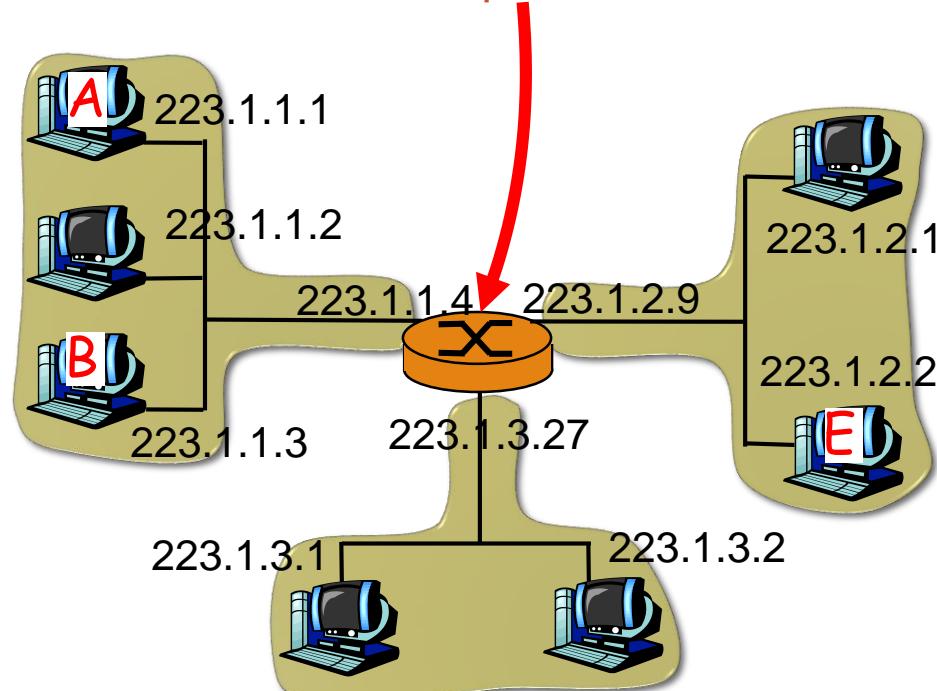
Levando um Datagrama da Fonte ao Destino

| | | | |
|--------------|-----------|-----------|-------|
| outro campos | 223.1.1.1 | 223.1.2.2 | dados |
|--------------|-----------|-----------|-------|

Chegando em 223.1.1.4,
destinado para 223.1.2.2

- examina endereço de rede de E
- E está na mesma rede da interface 223.1.2.9 do roteador
 - roteador e E estão diretamente ligados
- descobre endereço físico de 223.1.2.2 e envia o datagrama num quadro da camada de enlace
- datagrama chega em 223.1.2.2!!! (ufa!)

| Rede destino | Próx. roteador | Núm. saltos | Endereço Interface |
|--------------|----------------|-------------|--------------------|
| 223.1.1 | - | 1 | 223.1.1.4 |
| 223.1.2 | - | 1 | 223.1.2.9 |
| 223.1.3 | - | 1 | 223.1.3.27 |



Roteamento

Algoritmos de roteamento são descritos por grafos:

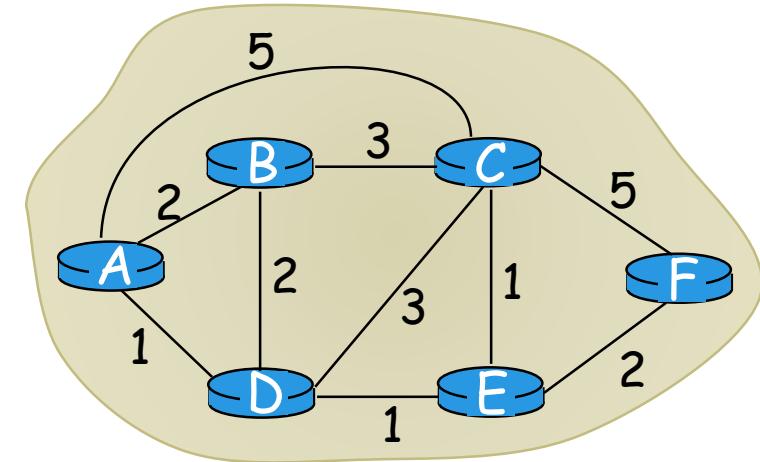
- Nós do grafo são roteadores
- Arestas do grafo são enlaces
- Custo do enlace: atraso, preço ou nível de congestionamento

Protocolo de Roteamento

OBJ: determinar “bons” caminhos (sequência de roteadores) através da rede da fonte ao destino.

□ “Bons” caminhos:

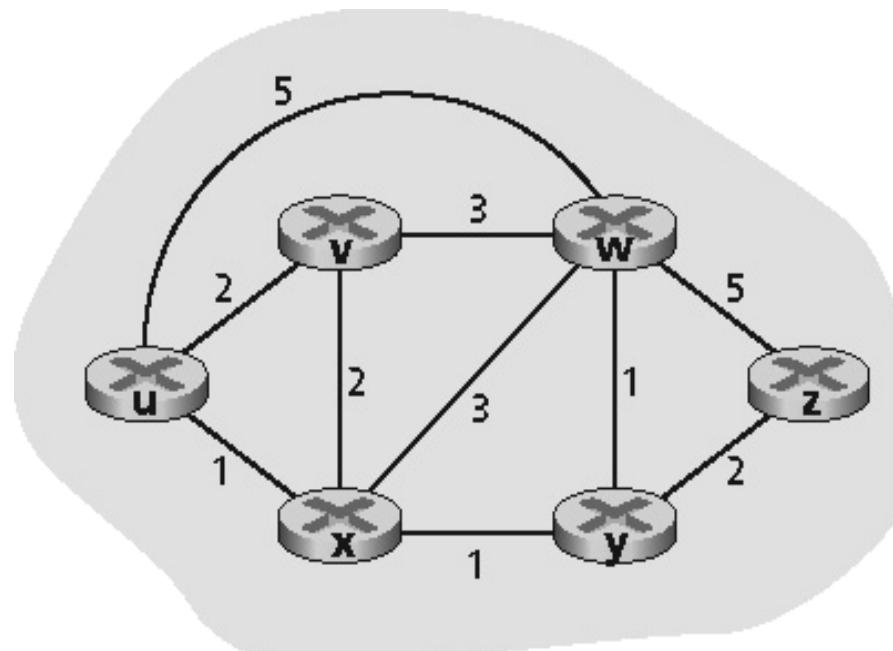
- tipicamente corresponde aos caminhos de menor custo
- caminhos redundantes



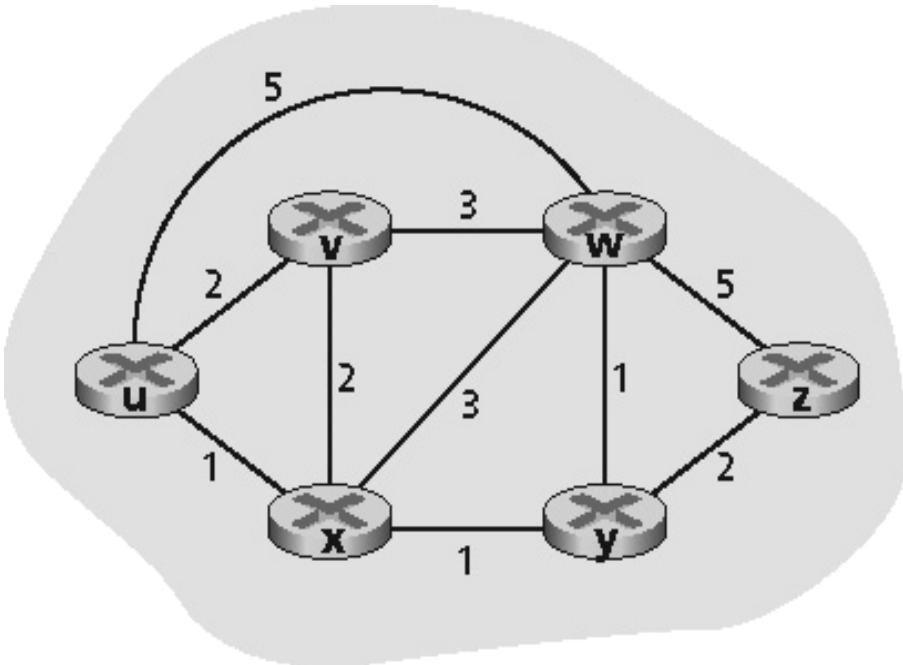
Abstração da Rede: Grafo

Grafo: $G = (N, E)$

- N = conjunto de roteadores
 $= \{ u, v, w, x, y, z \}$
- E = conjunto de enlaces
 $= \{ (u,v), (u,x), (v,x), (v,w), (x,w), (x,y), (w,y), (w,z), (y,z) \}$



Abstração da Rede: Custo



- $c(x, x')$ = custo do enlace (x, x')
 - ex., $c(w, z) = 5$
- Custo poderia ser sempre 1, ou proporcional ao congestionamento, ou inversamente relacionado à largura de banda

Custo do caminho $(x_1, x_2, x_3, \dots, x_p) = c(x_1, x_2) + c(x_2, x_3) + \dots + c(x_{p-1}, x_p)$

Questão: Qual é o caminho de menor custo entre u e z ?

Algoritmo de roteamento: algoritmo que encontra o caminho de menor custo

Roteamento

Algoritmos de roteamento

- Determinarão as melhores rotas
- Tipos: Link state, Distance vector
- Roteamento hierárquico

Protocolos de Roteamento: Definem formato das mensagens trocadas entre roteadores

- Para a execução dos algoritmos de roteamento
- Exemplos: RIP, OSPF, BGP

CAP 6. CAMADA DE REDE

AULA 9: ALGORITMOS DE ROTEAMENTO: LINK STATE E DISTANCE VECTOR

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

Algoritmos de roteamento

Algoritmos “link state”. Com Informação Global:

- Todos os roteadores têm informações completas da topologia e dos custos dos enlaces

Algoritmos “distance vector”. Com Informação Descentralizada:

- Roteadores só conhecem informações sobre seus vizinhos e os enlaces para eles
- Processo de computação iterativo
 - troca de informações com os vizinhos

Algoritmo de roteamento Link-State

Algoritmo de Dijkstra

- Topologia de rede e custo dos enlaces são conhecidos por todos os nós
 - Implementado via “link state broadcast”
 - Todos os nós (roteadores) têm a mesma informação
- Cada nó computa caminhos de menor custo deste nó para todos os outros nós
 - Fornece uma tabela de roteamento para aquele nó
- Convergência: após k iterações conhece o caminho de menor custo para k destinos (nós no grafo)

Algoritmo de roteamento Link-State

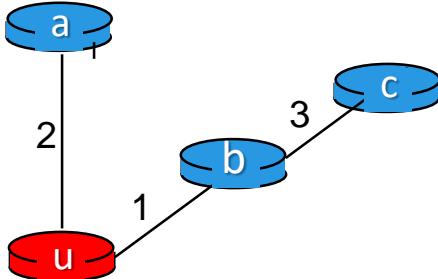
Notação no algoritmo de Dijkstra

- $C(i,j)$: custo do enlace do nó i ao nó j.
 - Custo é infinito se não houver ligação conhecida entre i e j
- $D(v)$: valor atual do custo do caminho da fonte ao destino v
- $P(v)$: nó predecessor ao longo do caminho da fonte ao nó v, isto é, antes do v
- N' : conjunto de nós cujo caminho de menor custo é definitivamente conhecido

Algoritmo de Dijkstra

1 Inicialização (rodando em um nó u):

```
2 N' = {u}  
3 para todos os nós v  
4   se v é adjacente a u  
5     então  $D(v) = c(u,v)$   
6     senão  $D(v) = \infty$   
7
```



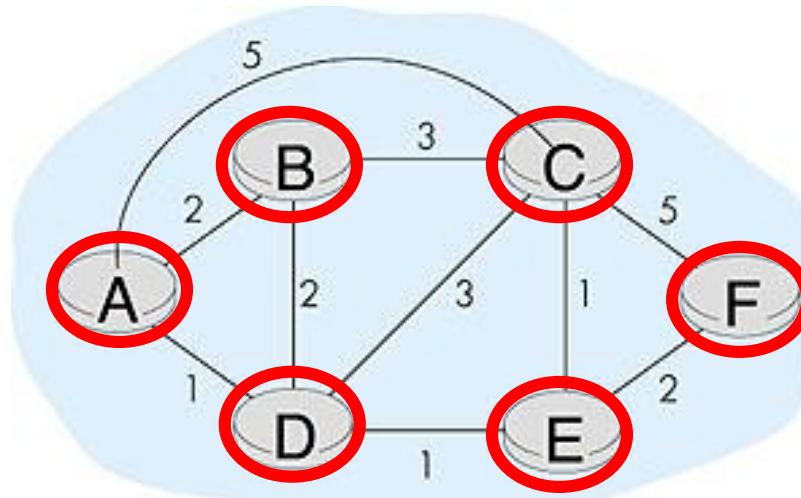
8 Loop

```
9   ache w não em N' tal que  $D(w)$  é um mínimo  
10  acrescente w a N'  
11  atualize  $D(v)$  para todo v adjacente a w e não em N':  
12     $D(v) = \min(D(v), D(w) + c(w,v))$   
13  /* novo custo para v é ou o custo anterior para v ou o menor  
14    custo do caminho conhecido para w mais o custo de w a v */  
15 até que todos os nós estejam em N'
```

```
2.  $N'=\{u\}$   
3-6:  $D(a)=2; D(b)=1; D(c)=\infty;$   
9:  $w=b$   
10:  $N'=\{u, b\}$   
11-12:  $D(c)=\min(\infty, 1+3)=4$   
9:  $w=a$   
10:  $N'=\{u, b, a\}$   
11: a não tem adjacente  
9:  $w=c$   
10:  $N'=\{u, b, a, c\}$   
No roteador u:  
-  $D(u)=0; D(a)=2; D(b)=1;$   
 $D(c)=4$ 
```

Exemplo: Algoritmo de Dijkstra

| Passo | N' | D(B),p(B) | D(C),p(C) | D(D),p(D) | D(E),p(E) | D(F),p(F) |
|-------|--------|-----------|-----------|-----------|-----------|-----------|
| → 0 | A | 2,A | 5,A | 1,A | ∞ | ∞ |
| → 1 | AD | 2,A | 4,D | | 2,D | ∞ |
| → 2 | ADE | 2,A | 3,E | | | 4,E |
| → 3 | ADEB | | 3,E | | | 4,E |
| → 4 | ADEBC | | | | | 4,E |
| → 5 | ADEBCF | | | | | |



Algoritmo de Dijkstra: exemplo

| Passo | N | D(B),p(B) | D(C),p(C) | D(D),p(D) | D(E),p(E) | D(F),p(F) |
|-------|--------|-----------|-----------|-----------|-----------|-----------|
| 0 | A | | 2,A | 5,A | 1,A | ∞ |
| 1 | AD | | 2,A | 4,D | | 2,D |
| 2 | ADE | | 2,A | 3,E | | 4,E |
| 3 | ADEB | | | 3,E | | 4,E |
| 4 | ADEBC | | | | | 4,E |
| 5 | ADEBCF | | | | | |

Árvore de caminhos mínimos resultante originada em A:

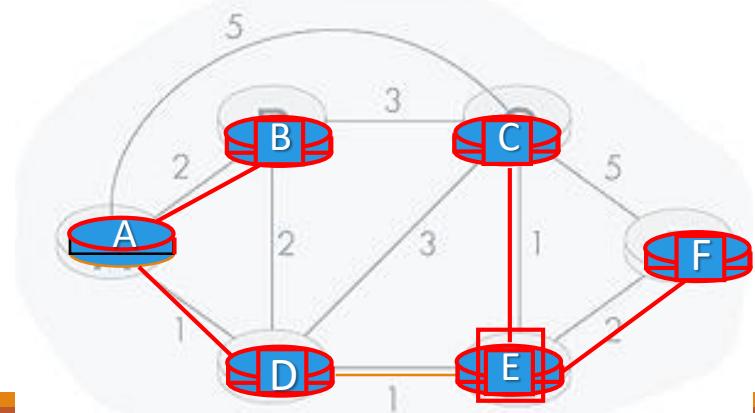


Tabela de encaminhamento resultante em A:

| destino | enlace |
|---------|--------|
| B | (A,B) |
| C | (A,D) |
| D | (A,D) |
| E | (A,D) |
| F | (A,D) |

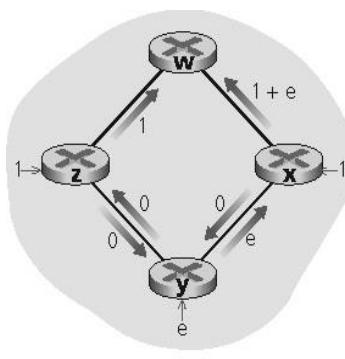
Discussão do algoritmo de Dijkstra

Complexidade do algoritmo: n nós

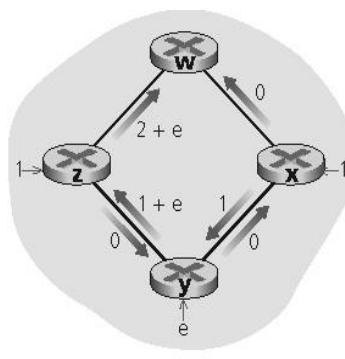
- Cada iteração: precisa verificar todos os nós w, que não estão em N'
 - 1a interação n nós, 2a interação n-1 nós, 3a interação n-2 nós,...
- Número de nós buscados em todas as interações: $n(n+1)/2$
- Complexidade: $O(n^2)$

Oscilações possíveis:

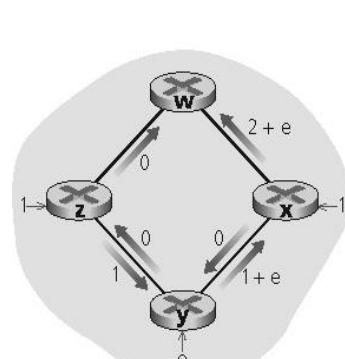
- Ex.: custo do enlace= quantidade de tráfego transportado



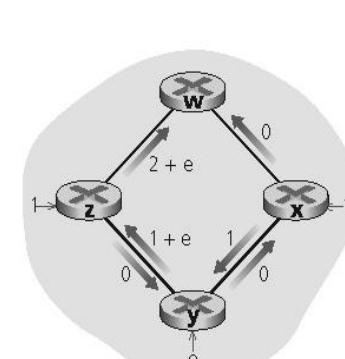
a. Roteamento inicial



b. x, y detectam melhor caminho até w em sentido horário



c. x, y, z detectam melhor caminho até w em sentido anti-horário

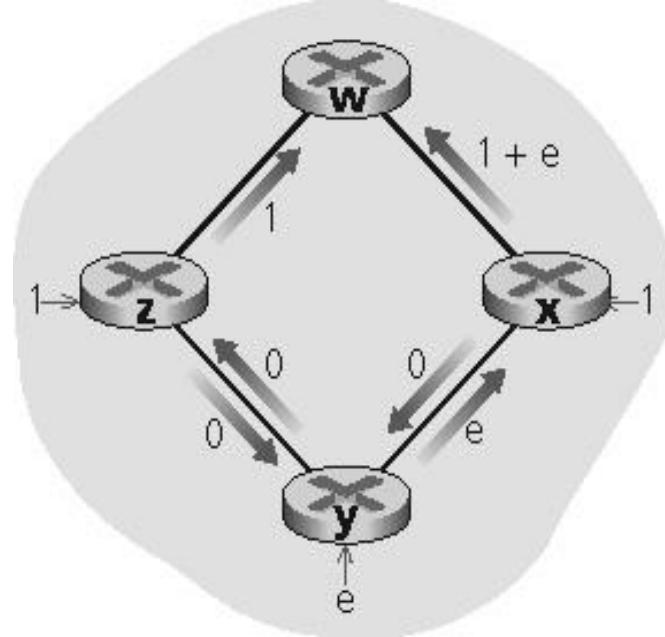


d. x, y, z, detectam melhor caminho até w em sentido horário

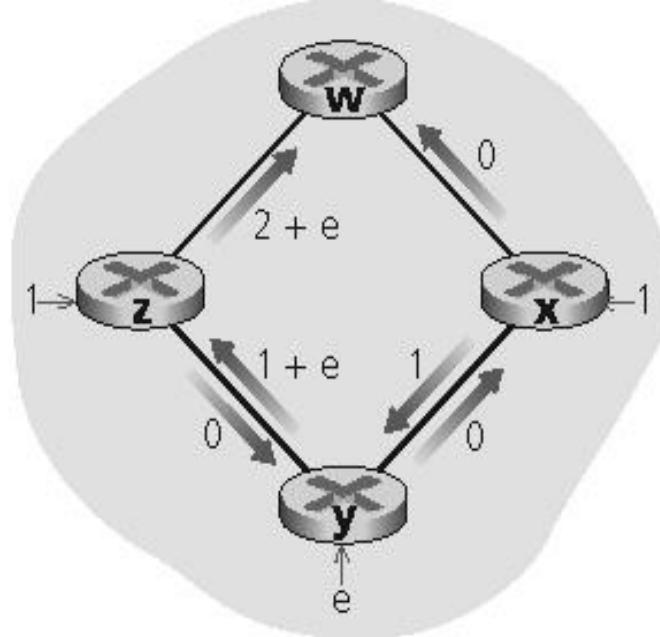
Discussão do algoritmo de Dijkstra

Oscilações possíveis:

- Ex.: custo do enlace = quantidade de tráfego transportado



a. Roteamento inicial

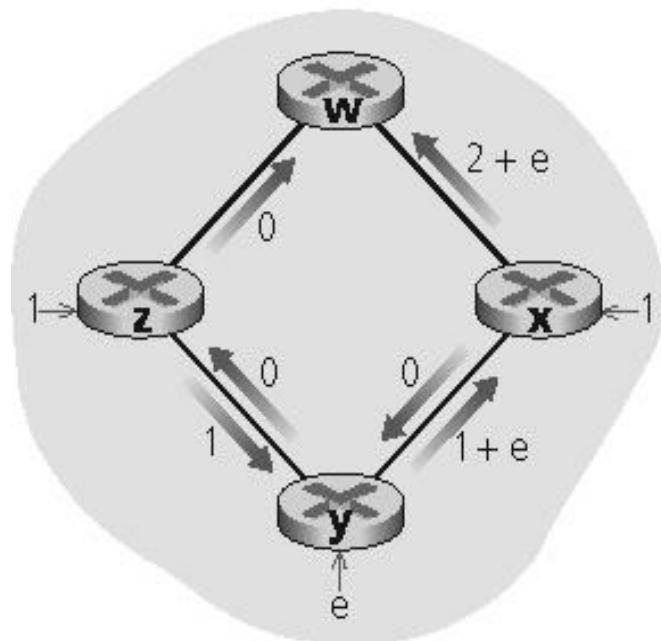


b. x, y detectam melhor caminho até w em sentido horário

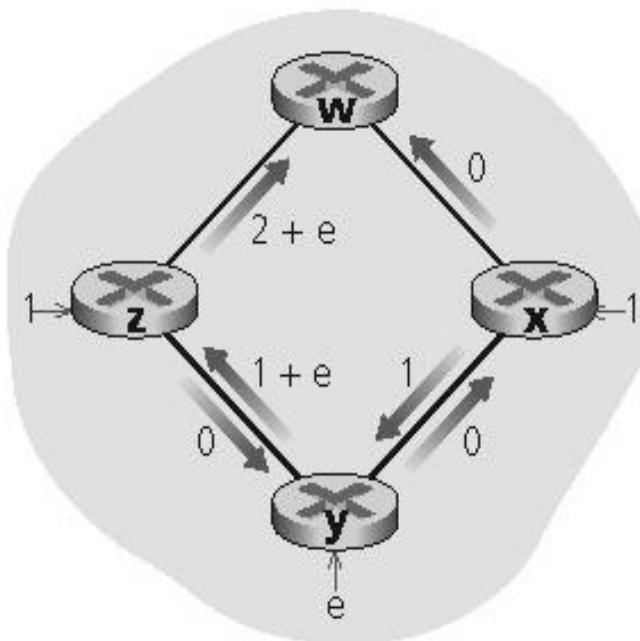
Discussão do algoritmo de Dijkstra

Oscilações possíveis:

- Ex.: custo do enlace = quantidade de tráfego transportado



c. x, y, z detectam melhor caminho até w em sentido anti-horário

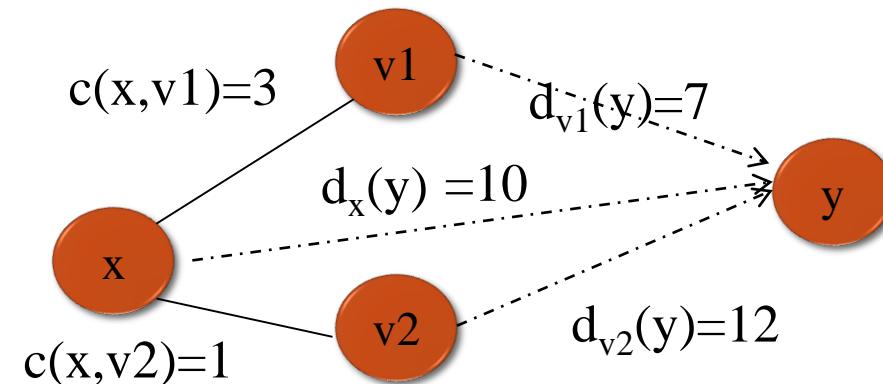


d. x, y, z , detectam melhor caminho até w em sentido horário

Algoritmo vetor de distância (1)

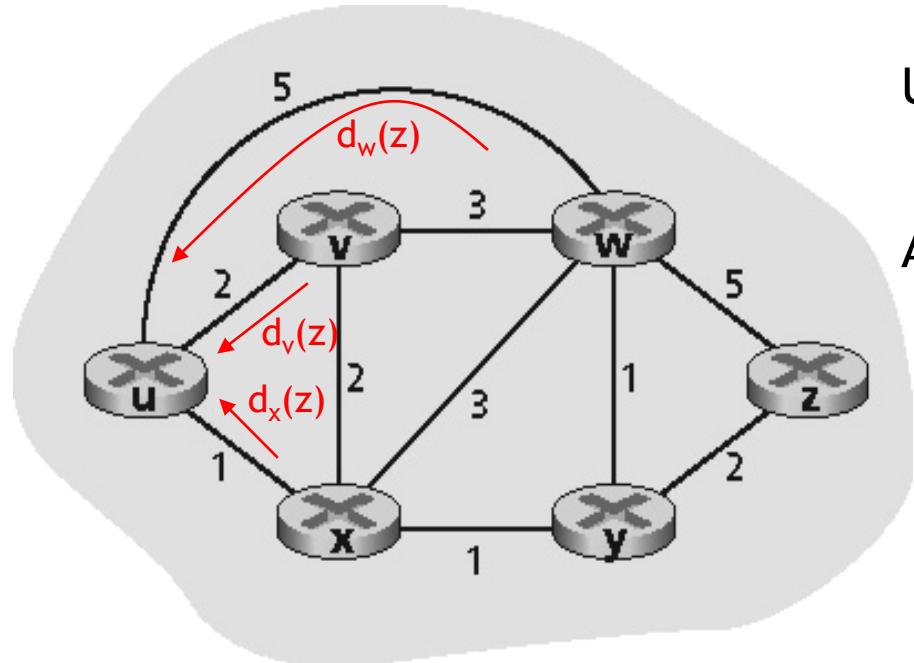
Equação de Bellman-Ford (programação dinâmica)

- Define
 - $d_x(y) = \text{custo do caminho de menor custo de } x \text{ para } y$
- Então
 - $d_x(y) = \min_v \{c(x,v) + d_v(y)\}$
 - Em que \min_v é calculado para todos os vizinhos de x
 - No exemplo: $d_x(y) = \min_v \{c(x,v1) + d_{v1}(y), c(x,v2) + d_{v2}(y)\}$



Exemplo: Bellman-Ford (2)

Exemplo: custo entre o nó u e o nó z



U recebe a informação dos vizinhos:

$$d_v(z) = 5, d_x(z) = 3, d_w(z) = 3$$

A equação B-F diz que:

$$\begin{aligned} d_u(z) &= \min \{ c(u,v) + d_v(z), \\ &\quad c(u,x) + d_x(z), \\ &\quad c(u,w) + d_w(z) \} \\ &= \min \{ 2 + 5, \\ &\quad 1 + 3, \\ &\quad 5 + 3 \} = 4 \end{aligned}$$

Caminho mínimo $d_u(z) = 4$
passando por x

O nó que atinge o mínimo é o próximo salto no caminho mais curto
→ tabela de roteamento

Algoritmo vetor de distância (3)

Define a forma de comunicação de vizinho para vizinho

- Atualizando a tabela de roteamento para que o pacote seja enviado para o vizinho no caminho de menor custo

Cada nó x mantém os seguintes dados de roteamento

- Para cada vizinho v, ele mantém o custo $c(x,v)$
- O vetor de distâncias (DV) do nó x
 - $Dx = [Dx(y): y \in N]$
- Os vetores de distância de seus vizinhos
 - Para cada vizinho v, x mantém $Dv = [Dv(y): y \in N]$

Algoritmo vetor de distância (4)

Idéia básica:

- Cada nó envia periodicamente sua própria estimativa de vetor de distâncias aos vizinhos
- Quando o nó x recebe nova estimativa de DV do vizinho, ele atualiza seu próprio DV usando a equação B-F:
 - $Dx(y) = \min_v \{c(x,v) + Dv(y)\}$ para cada nó $y \in N$
- Ao menos em condições naturais, a estimativa $Dx(y)$ converge para o menor custo atual $d_x(y)$

Algoritmo vetor de distância

Tabela do nó x

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | 0 | 2 | 7 |
| | y | ∞ | ∞ | ∞ |
| | z | ∞ | ∞ | ∞ |

DV do Nó

DVs dos vizinhos

Tabela do nó y

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | 2 | 0 | 1 |
| | z | ∞ | ∞ | ∞ |

DV do Nó

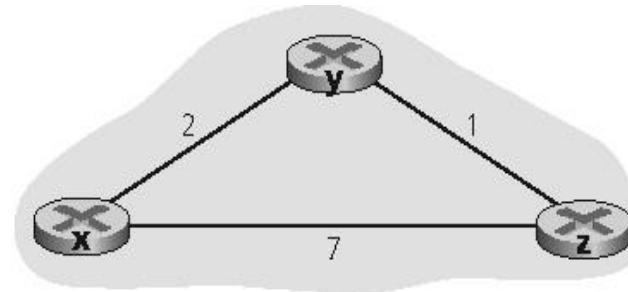
DVs dos vizinhos

Tabela do nó z

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | ∞ | ∞ | ∞ |
| | z | 7 | 1 | 0 |

DVs dos vizinhos

DV do nó



Algoritmo vetor de distância

Tabela do nó x

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | 0 | 2 | 7 |
| | y | ∞ | ∞ | ∞ |
| | z | ∞ | ∞ | ∞ |

$$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\}$$

$$= \min\{2+0, 7+1\} = 2$$

$$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\}$$

$$= \min\{2+1, 7+0\} = 3$$

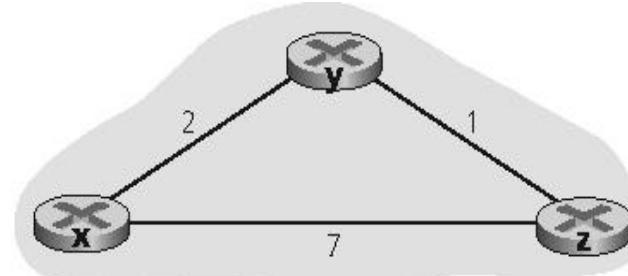
Tabela do nó y

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | 2 | 0 | 1 |
| | z | ∞ | ∞ | ∞ |

Tabela do nó z

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | ∞ | ∞ | ∞ |
| | z | 7 | 1 | 0 |

Tempo



Algoritmo vetor de distância

Tabela do nó x

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | 0 | 2 | 7 |
| | y | ∞ | ∞ | ∞ |
| | z | 8 | 8 | 8 |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 3 |
| | y | 2 | 0 | 1 |
| | z | 7 | 1 | 0 |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 3 |
| | y | 2 | 0 | 1 |
| | z | 3 | 1 | 0 |

Tabela do nó y

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | 2 | 0 | 1 |
| | z | ∞ | ∞ | ∞ |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 7 |
| | y | 2 | 0 | 1 |
| | z | 7 | 1 | 0 |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 3 |
| | y | 2 | 0 | 1 |
| | z | 3 | 1 | 0 |

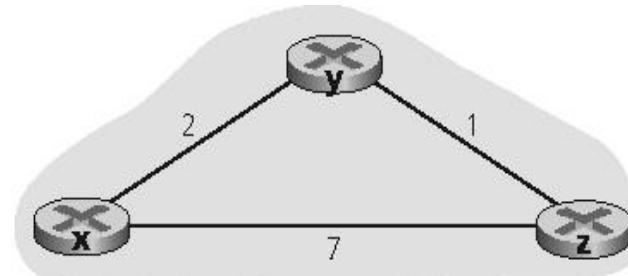
Tabela do nó z

| | | Custo até | | |
|----|---|-----------|----------|----------|
| | | x | y | z |
| De | x | ∞ | ∞ | ∞ |
| | y | ∞ | ∞ | ∞ |
| | z | 7 | 1 | 0 |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 7 |
| | y | 2 | 0 | 1 |
| | z | 3 | 1 | 0 |

| | | Custo até | | |
|----|---|-----------|---|---|
| | | x | y | z |
| De | x | 0 | 2 | 3 |
| | y | 2 | 0 | 1 |
| | z | 3 | 1 | 0 |

Tempo



Algoritmo vetor de distância (5)

Iterativo, assíncrono: cada iteração local é causada por:

- Mudança no custo do enlace local
- Mensagem de atualização DV do vizinho

Distribuído:

- Cada nó notifica os vizinhos apenas quando seu DV mudar
- Os vizinhos então notificam seus vizinhos, se necessário

Cada nó:

espera por (mudança no custo do enlace local na mensagem do vizinho)

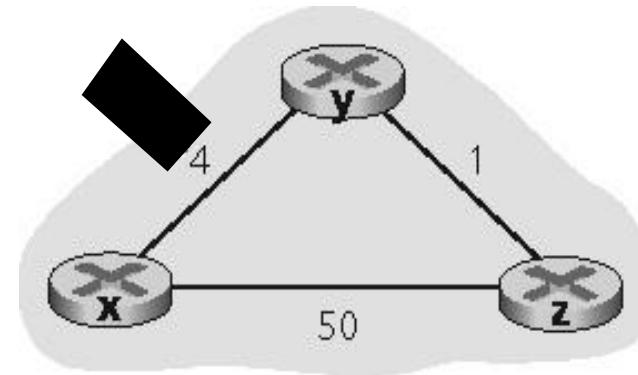
recalcula estimativas

se o DV para qualquer destino mudou, notifica os vizinhos

Vetor de distância: mudanças no custo do enlace

Mudanças no custo do enlace:

- Nó detecta mudança no custo do enlace local
- Atualiza informações de roteamento, recalcula o vetor de distância
- Se o DV muda, notifica vizinhos



a.

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó X (inicial)

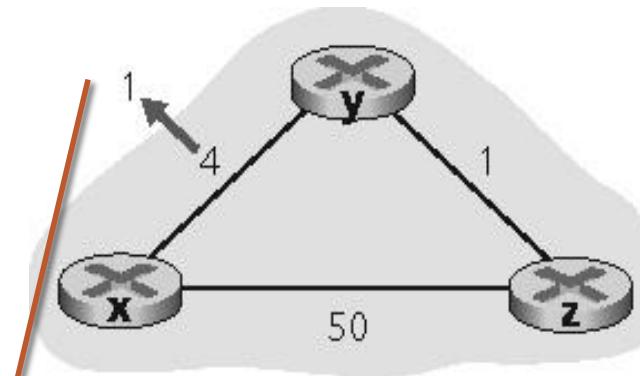
| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó y (inicial)

Vetor de distância: mudanças no custo do enlace

Mudanças no custo do enlace:

- Nó detecta mudança no custo do enlace local
- Atualiza informações de roteamento, recalcula o vetor de distância
- Se o DV muda, notifica vizinhos



a.

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó X (inicial)

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 1 | 0 | 1 |
| | z | 5 | 1 | 0 |

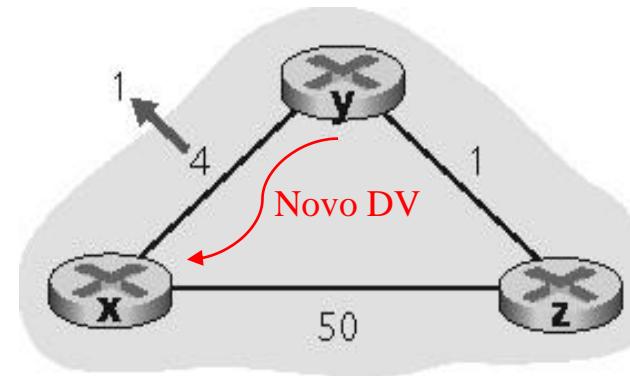
Nó y (custo reduzido)

$$\begin{aligned} D_y(x) &= \min\{c(y,x)+D_x(x), \\ &\quad c(y,z)+D_z(x)\} \\ &= \min \{1+0, 1+50\} = 1 \end{aligned}$$

Vetor de distância: mudanças no custo do enlace

Mudanças no custo do enlace:

- Nó detecta mudança no custo do enlace local
- Atualiza informações de roteamento, recalcula o vetor de distância
- Se o DV muda, notifica vizinhos



| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 1 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó X (recebe novo custo)

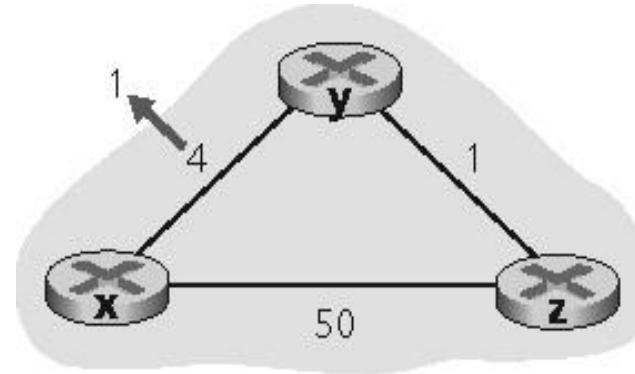
| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 1 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó y (custo reduzido)

Vetor de distância: mudanças no custo do enlace

Mudanças no custo do enlace:

- Nó detecta mudança no custo do enlace local
- Atualiza informações de roteamento, recalcula o vetor de distância
- Se o DV muda, notifica vizinhos



a.

“boas notícias viajam depressa”

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 1 | 2 |
| | y | 1 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó X (recalcula DV)

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 1 | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó y (custo reduzido)

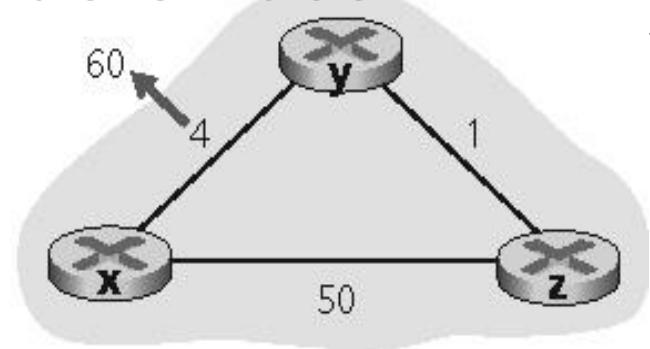
$$\begin{aligned} D_x(y) &= \min\{c(x,y)+D_y(y), \\ &\quad c(x,z)+D_z(y)\} \\ &= \min\{1+0,50+1\} = 1 \end{aligned}$$

$$\begin{aligned} D_x(z) &= \min\{c(x,y)+D_y(z), \\ &\quad c(x,z)+D_z(z)\} \\ &= \min\{1+1,50+0\} = 2 \end{aligned}$$

Vetor de distância: mudanças no custo do enlace

Mudanças no custo do enlace:

- Boas notícias viajam rápido
- Más notícias viajam devagar — problema da “contagem ao infinito”!



b.

$$\begin{aligned}D_y(x) &= \min\{c(y,x) + D_x(x), \\&\quad c(y,z) + D_z(x)\} \\&= \min\{60+0, 1+5\} \\&= 6 \text{ passando por } z\end{aligned}$$

| | | Até | | | |
|----------------|---|-----|---|---|--|
| | | x | y | z | |
| De | x | 0 | 4 | 5 | |
| | y | 4 | 0 | 1 | |
| | z | 5 | 1 | 0 | |
| Nó x (inicial) | | Até | | | |
| De | | x | y | z | |
| De | x | 0 | 4 | 5 | |
| | y | 4 | 0 | 1 | |
| | z | 5 | 1 | 0 | |
| Nó y (inicial) | | Até | | | |
| De | | x | y | z | |
| De | x | 0 | 4 | 5 | |
| | y | 4 | 0 | 1 | |
| | z | 5 | 1 | 0 | |
| Nó z (inicial) | | Até | | | |
| De | | x | y | z | |

Vetor de distância: mudanças no custo do enlace

Y detecta a mudança de custo

- $D_y(x) = \min\{c(y,x) + D_x(x), c(y,z) + D_z(x)\} = \min\{60, 6\} = 6$
- Um equivoco! Gera um loop de roteamento

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

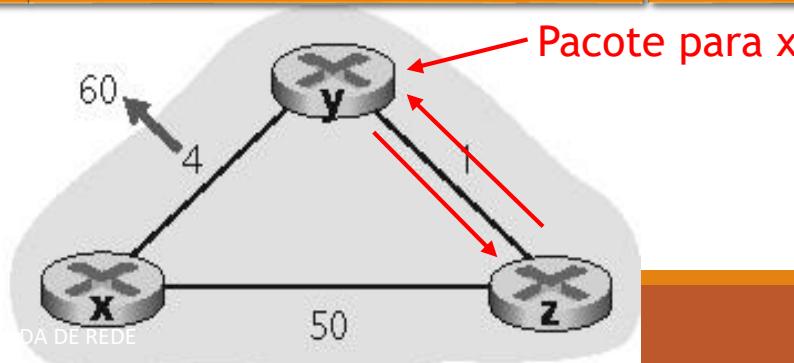
Nó x (inicial)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 6 (z) | 0 | 1 |
| | z | 5 (y) | 1 | 0 |

Nó y (detecta mudança)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 4 | 0 | 1 |
| | z | 5 (y) | 1 | 0 |

Nó z (inicial)



Vetor de distância: mudanças no custo do enlace

Atualizando DV, y informa a z

- Y informa que $Dy(x)=6$ e como z sabe que $c(z,y)=1$, então $Dz(x)=7$
- Z informa novo DV a y

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

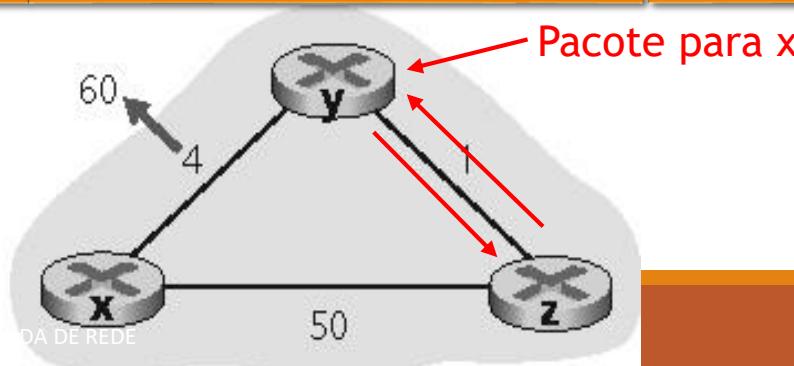
Nó x (inicial)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 6 (z) | 0 | 1 |
| | z | 5 | 1 | 0 |

Nó y (detecta mudança)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 6 (z) | 0 | 1 |
| | z | 7 (y) | 1 | 0 |

Nó z (atualizando)



Vetor de distância: mudanças no custo do enlace

Atualizando DV, z informa a y

- z informa que $Dz(x)=7$ e como y sabe que $c(y,z)=1$, então $Dy(x)=8$
- y informa novo DV a z

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

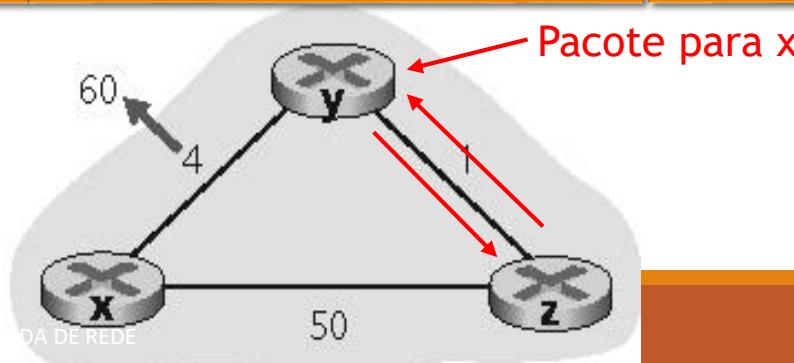
Nó x (inicial)

| | | Até | | |
|----|---|------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 8(z) | 0 | 1 |
| | z | 7(y) | 1 | 0 |

Nó y (atualizando)

| | | Até | | |
|----|---|------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | y | 6(z) | 0 | 1 |
| | z | 7(y) | 1 | 0 |

Nó z (atualizado)



Vetor de distância: mudanças no custo do enlace

44 iterações antes de o algoritmo estabilizar!!!

| | | Até | | |
|----|---|-----|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 4 | 0 | 1 |
| | z | 5 | 1 | 0 |

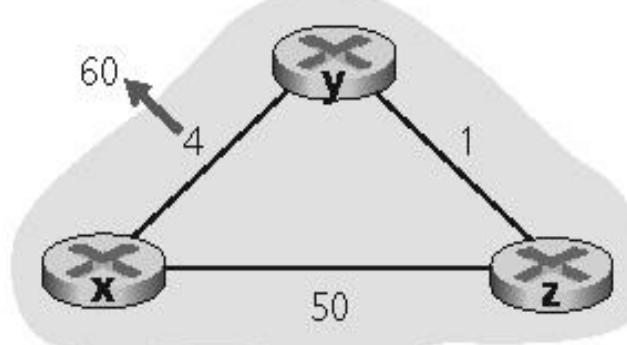
Nó x (inicial)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 8 (z) | 0 | 1 |
| | z | 7 (y) | 1 | 0 |

Nó y (atualizado)

| | | Até | | |
|----|---|-------|---|---|
| | | x | y | z |
| De | x | 0 | 4 | 5 |
| | Y | 8 (z) | 0 | 1 |
| | z | 7 (y) | 1 | 0 |

Nó z (atualizando)



b.

Vetor de distância: mudanças no custo do enlace

44 iterações antes de o algoritmo estabilizar!!!

| | | Até | | |
|----|---|-----|----|----|
| | | x | y | z |
| De | x | 0 | 51 | 50 |
| | Y | 51 | 0 | 1 |
| | z | 50 | 1 | 0 |

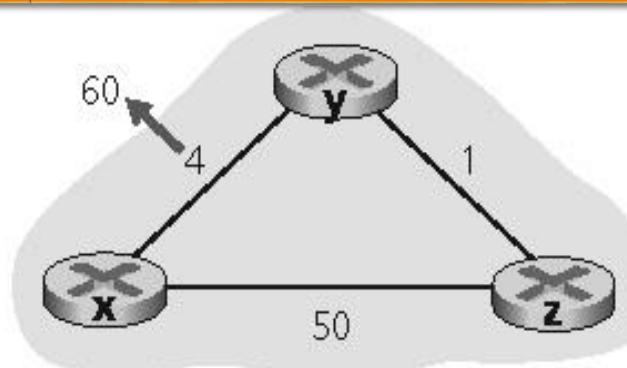
Nó x (inicial)

| | | Até | | |
|----|---|-----|----|----|
| | | x | y | z |
| De | x | 0 | 51 | 50 |
| | Y | 51 | 0 | 1 |
| | z | 50 | 1 | 0 |

Nó y (atualizado)

| | | Até | | |
|----|---|-----|----|----|
| | | x | y | z |
| De | x | 0 | 51 | 50 |
| | Y | 51 | 0 | 1 |
| | z | 50 | 1 | 0 |

Nó z (atualizando)



b.

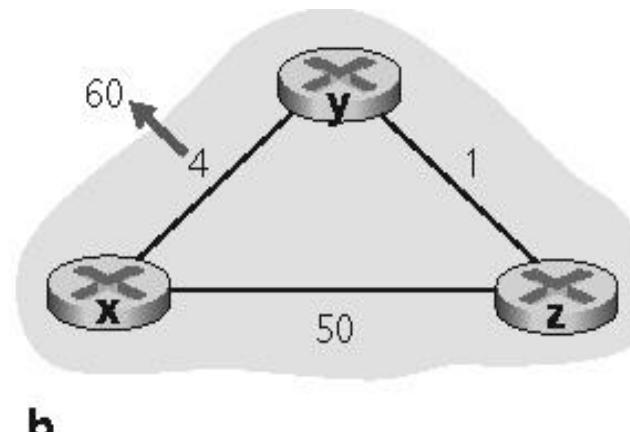
Vetor de distância: mudanças no custo do enlace

Solução: Reversão envenenada:

- Se Z roteia por Y para alcançar X :
 - Z diz a Y que sua distância (de Z) para X é infinita (então Y não roteará até X via Z)

Isso resolverá completamente o problema da contagem ao infinito?

- Não é solução geral para loops envolvendo três ou mais nós



Comparação dos algoritmos LS e VD

Complexidade

- LS: com n nós, E links, $O(NE)$ mensagens enviadas
- DV: trocas somente entre vizinhos - Tempo de convergência varia

Tempo de convergência

- LS: algoritmo $O(N^2)$ exige mensagens $O(NE)$
 - Pode ter oscilações
- DV: tempo de convergência varia
 - Pode haver loops de roteamento durante a convergência
 - Problema da contagem ao infinito

Comparação dos algoritmos LS e VD

Robustez: o que acontece se um roteador funciona mal?

- LS:
 - Nós podemos informar custos de link incorretos
 - Cada nó calcula sua própria tabela de roteamento: aumenta a robustez
- DV:
 - Nó DV pode informar custo de caminho incorreto
 - Tabela de cada nó é usada por outros
 - Propagação de erros pela rede

Pontos Importantes

Algoritmo Link State e Distance Vector

- Entender princípios gerais
- Saber comparar algoritmos: vantagens e deficiências

CAP 6. CAMADA DE REDE

AULA 10: PROTOCOLOS RIP E OSPF

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

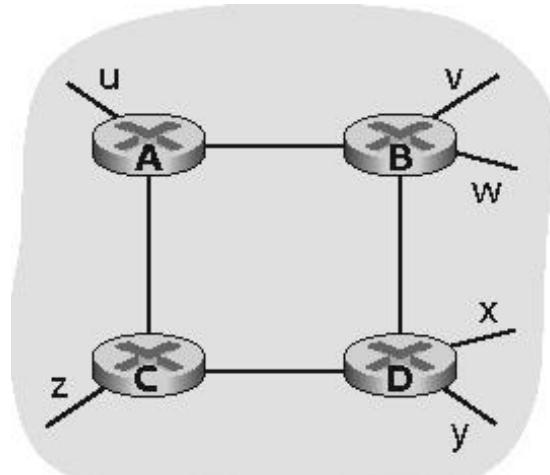
ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://MOODLE.UFSC.BR)

RIP (Routing Information Protocol)

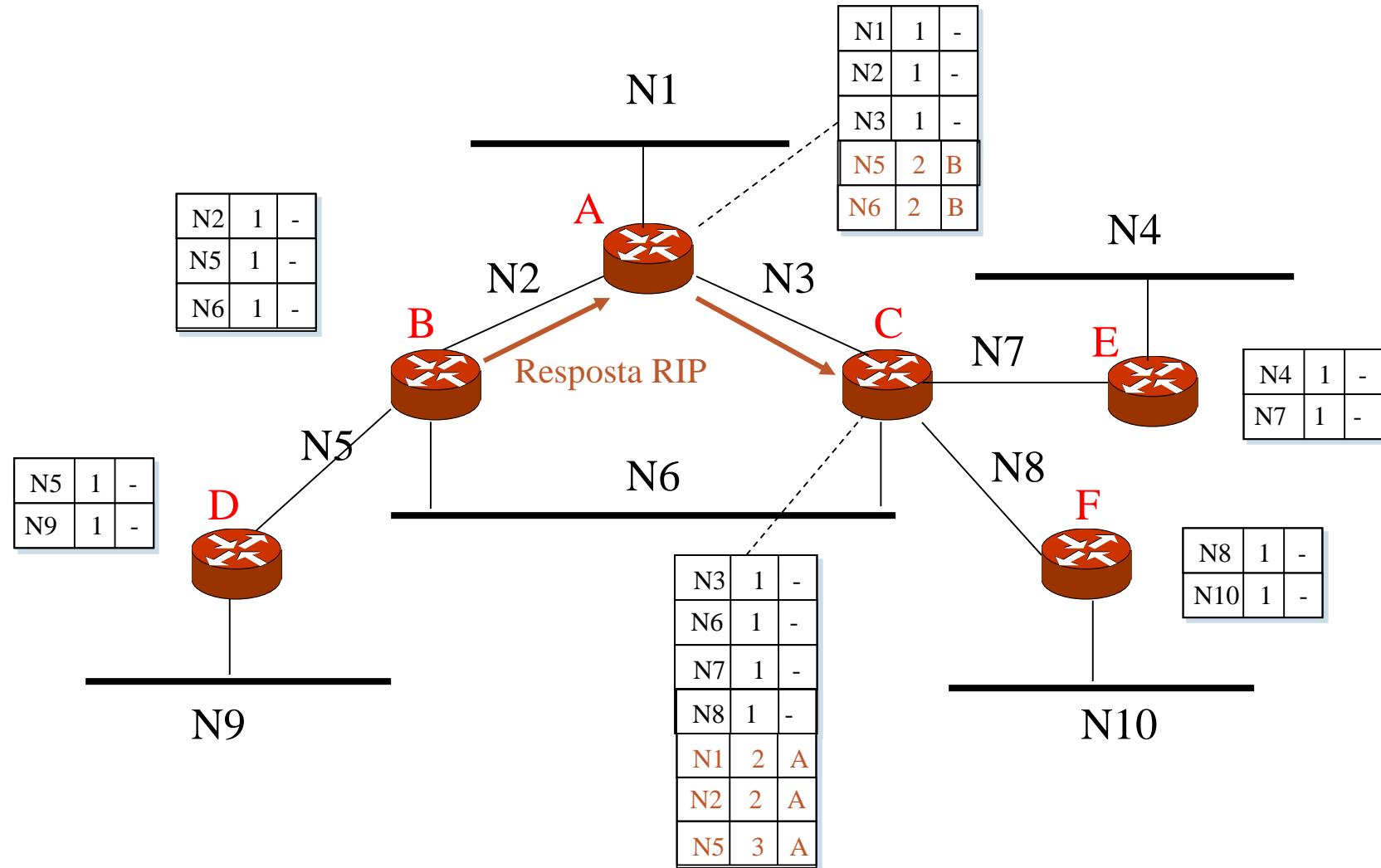
RIP-1 (RFC 1058), RIP-2 (RFC 1388)

- Utiliza o algoritmo Distance Vector
- Métrica do custo é a distância: calculada através da soma do número de roteadores existentes no caminho (# de hops, max=15 hops)
 - 1: Diretamente conectado
 - 16: infinito
- RIP não pode suportar redes com diâmetro > 15.

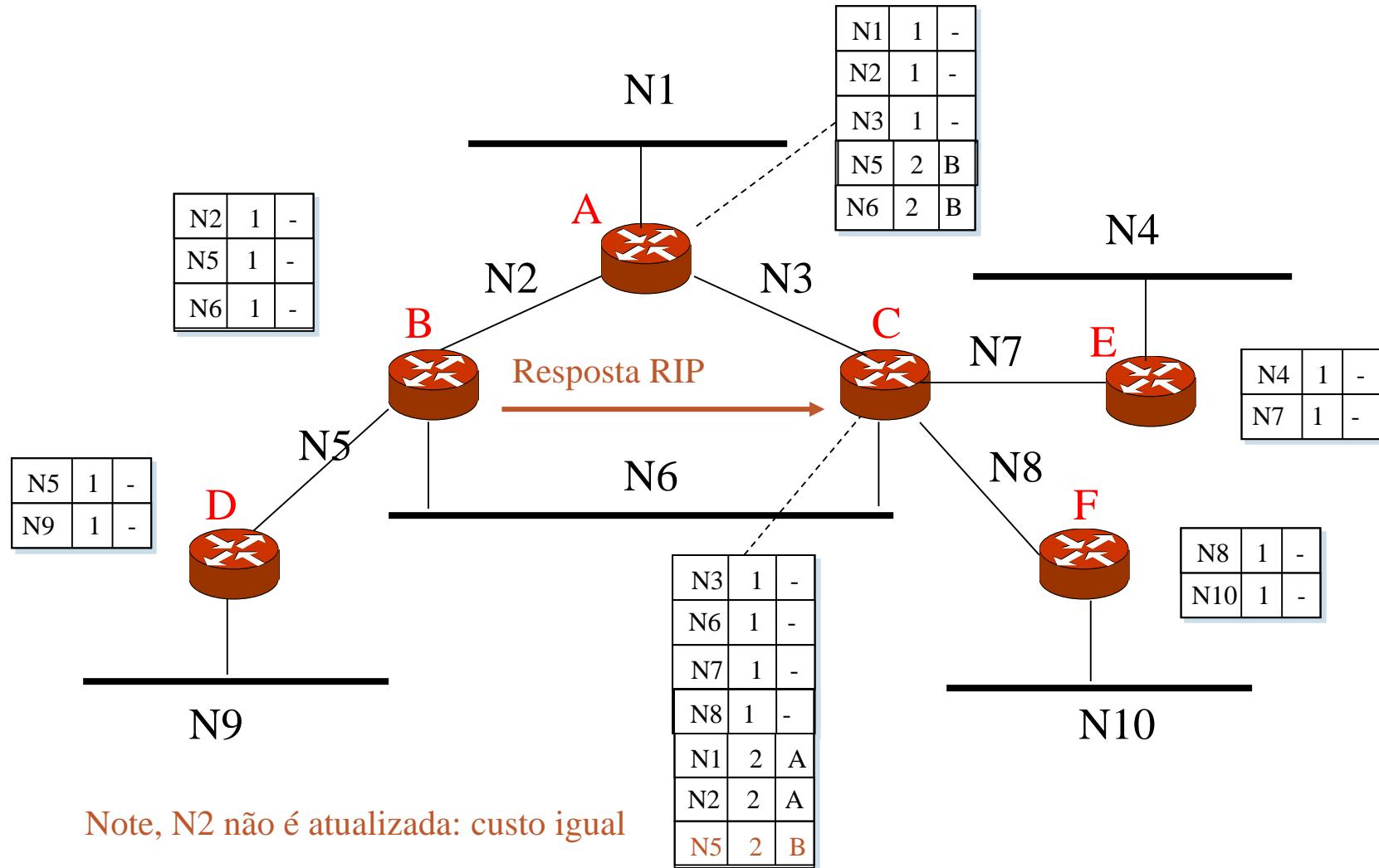


| Destino | Saltos |
|---------|--------|
| u | 1 |
| v | 2 |
| w | 2 |
| x | 3 |
| y | 3 |
| z | 2 |

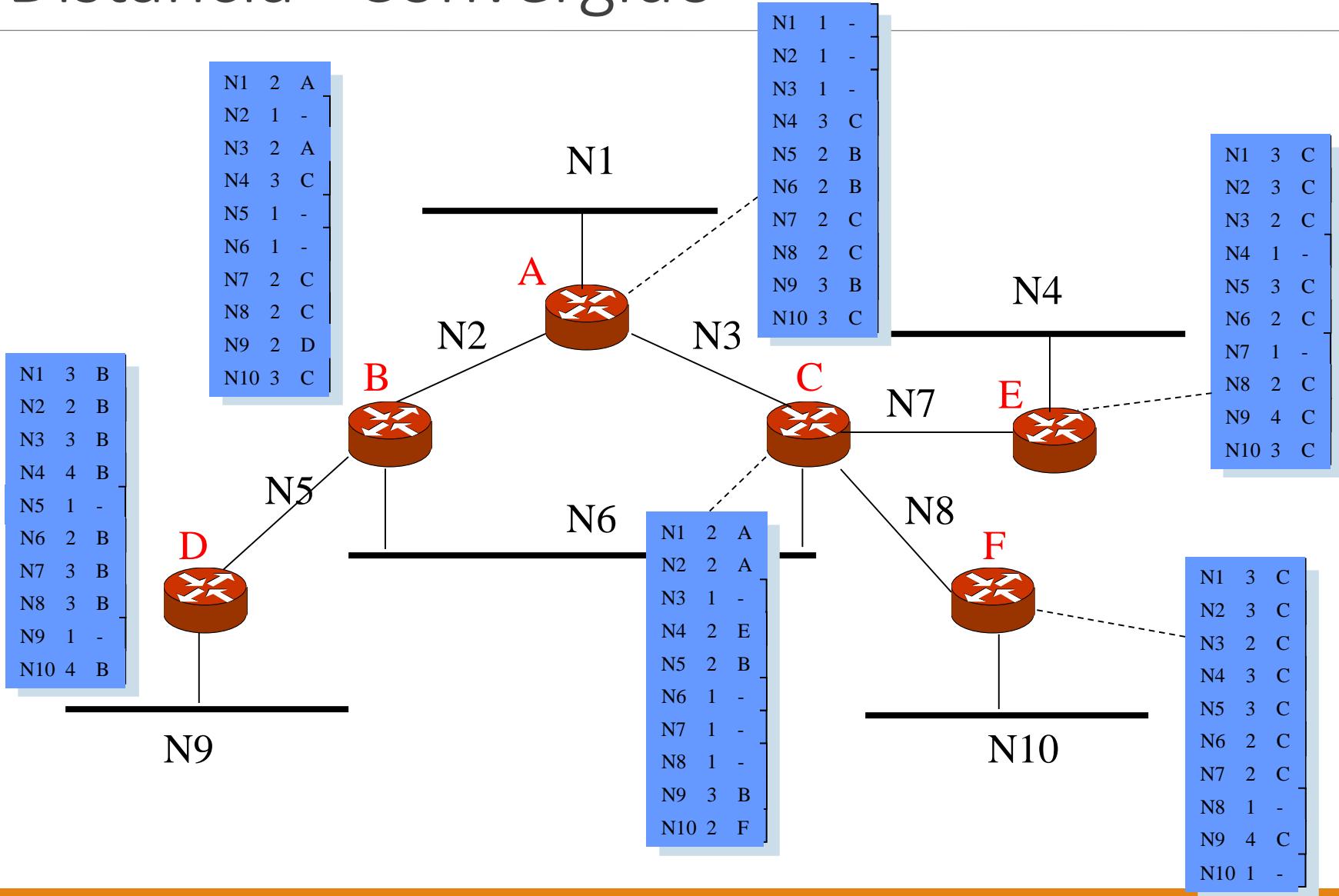
RIP: Vetor de Distância



Vetor Distância



Vetor Distância - Convergido



RIP

RIP usa vetor de distâncias

- Todo nó envia suas tabelas de rotas para seus vizinhos
 - A cada 30 segundos via Response Message (anúncio)
 - Contendo a rota e o custo (número de hops)
 - Informações de rota gradualmente se espalham através da rede
 - Todo nó seleciona a rota com a menor métrica

Mensagens rip são enviadas via datagramas UDP

- IP Multicast (RIP-2) or Broadcast (RIP-1)

RIP: falha de enlaces e recuperação

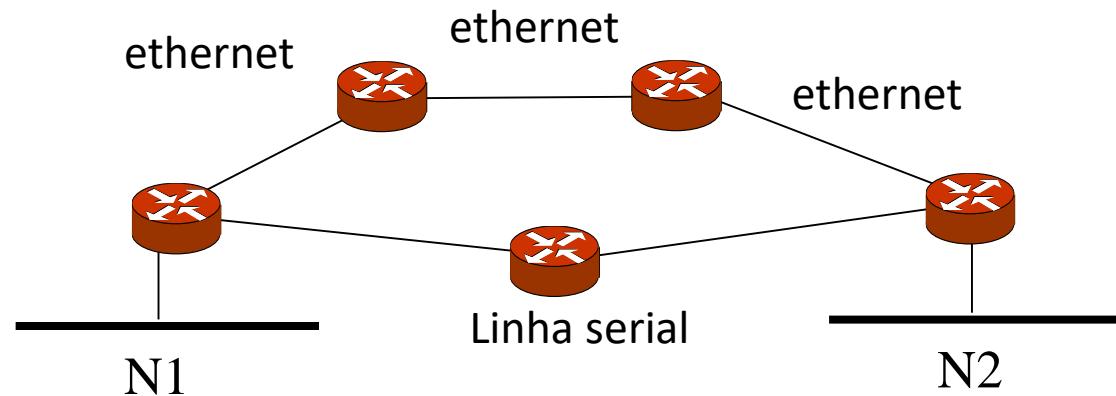
Se não há um aviso depois de 180 s, --> o vizinho e o enlace são declarados mortos

- Rotas através do vizinho são anuladas
- Novos anúncios são enviados aos vizinhos
- Os vizinhos por sua vez devem enviar novos anúncios (se suas tabelas de rotas foram alteradas)
- A falha de um enlace se propaga rapidamente para a rede inteira
- Reversão envenenada é usada para prevenir loops,
(distância infinita = 16 saltos)

Problemas do RIP

Uso de contagem de hosts pode não ser a métrica adequada para definir a rota de menor custo

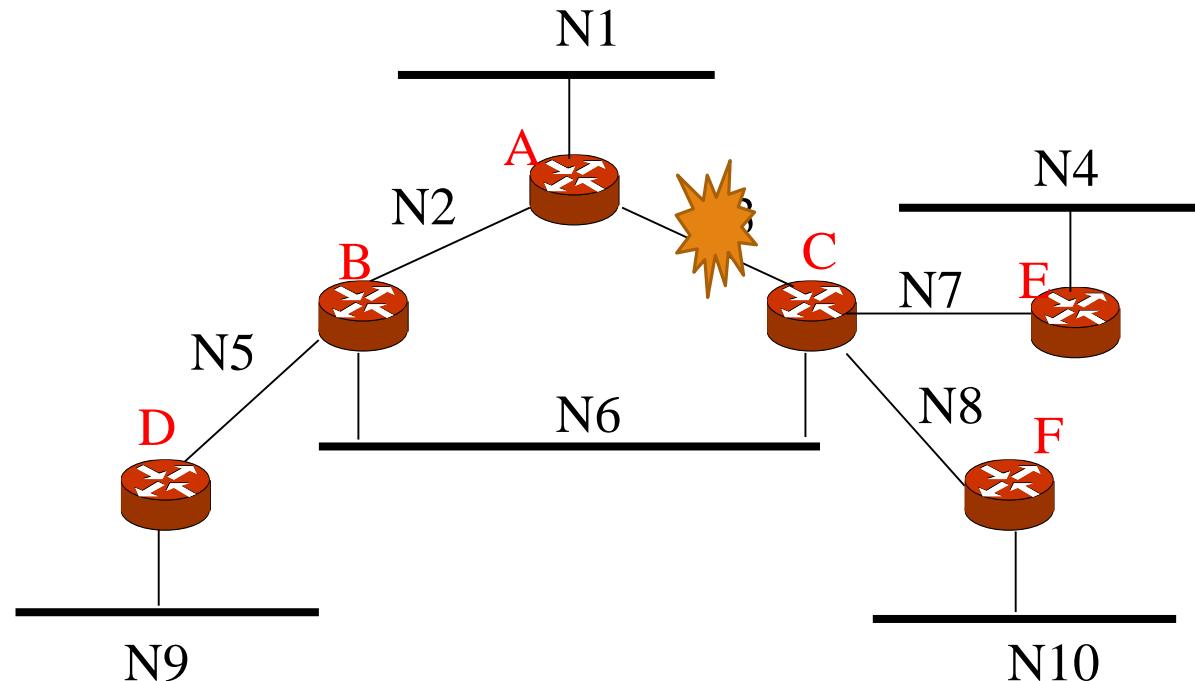
- Nem sempre traz bons resultados
 - # saltos = 3 passando por Ethernets
 - # saltos = 2 passando por linhas seriais lentas!
- Muitas implementações do RIP permitem que o gerenciador sete artificialmente os custos



Problemas do RIP

Após a falha de uma rota ou link

- RIP pode levar minutos para estabilizar
- Cada vizinho fala apenas todo 30s
- O tempo para a informação propagar por vários hops é na ordem de minutos



Problemas do RIP

A métrica máxima útil é 15

- Diâmetro da rede dever ser menor ou igual a 15

RIP usa muita largura de banda

- Ele envia tabelas de roteamento completas para atualizações

OSPF: Open Shortest Path First

Protocolo recomendado pela IETF

- Desenvolvido para substituir o RIP (1988-1991)
- OPEN por ser um padrão aberto
- Utiliza Link State (Algoritmo de Dijkstra)

OSPF usa IP diretamente (Campo Protocol = 89)

- Não usa UDP ou TCP.
- Usa multicast

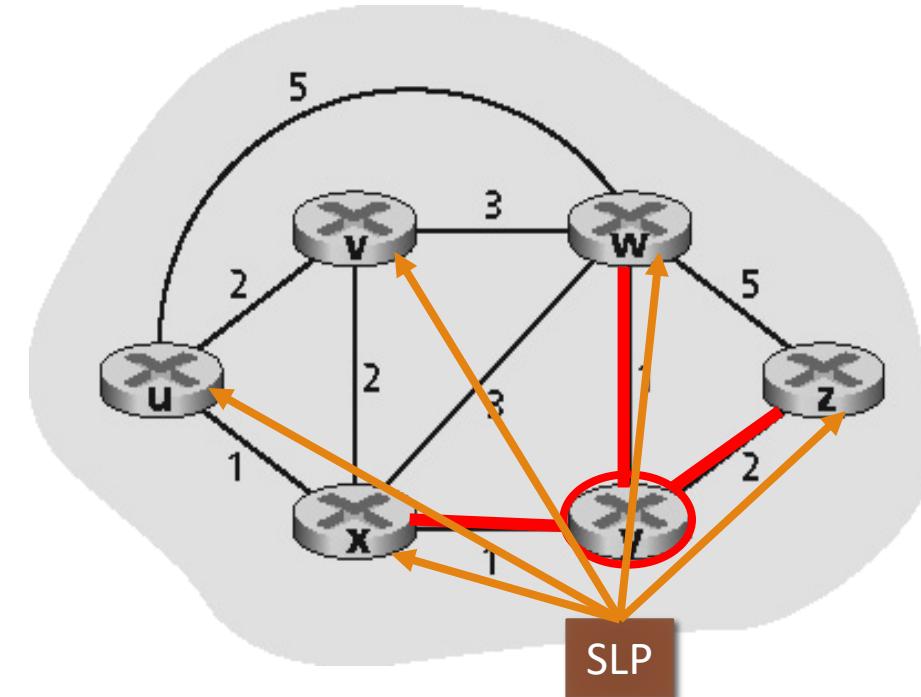
OSPF: Protocolo Link-State (SPF)

No SPF, todo roteador faz o seguinte:

- Testa periodicamente o status de todos os vizinhos
 - Constrói um pacote Link State (LSP) com esta informação e propaga para todos os outros roteadores
- Usando LSPs vindo de todos os outros roteadores, cada roteador computa uma árvore de envio de caminho de menor custo usando o algoritmo de Dijkstra.

Vantagens (sobre o vetor de distância):

- Mais funcionalidade devido ao cálculo na origem do dado e não dependência dos roteadores intermediários
- Conhecimento da topologia completa
- Facilidade de recuperação de falhas
- Convergência rápida



OSPF : Protocolo Link-State (SPF)

Especifica que toda troca de informações entre roteadores seja autenticada

- Apenas roteadores confiáveis difundem as informações sobre o roteamento

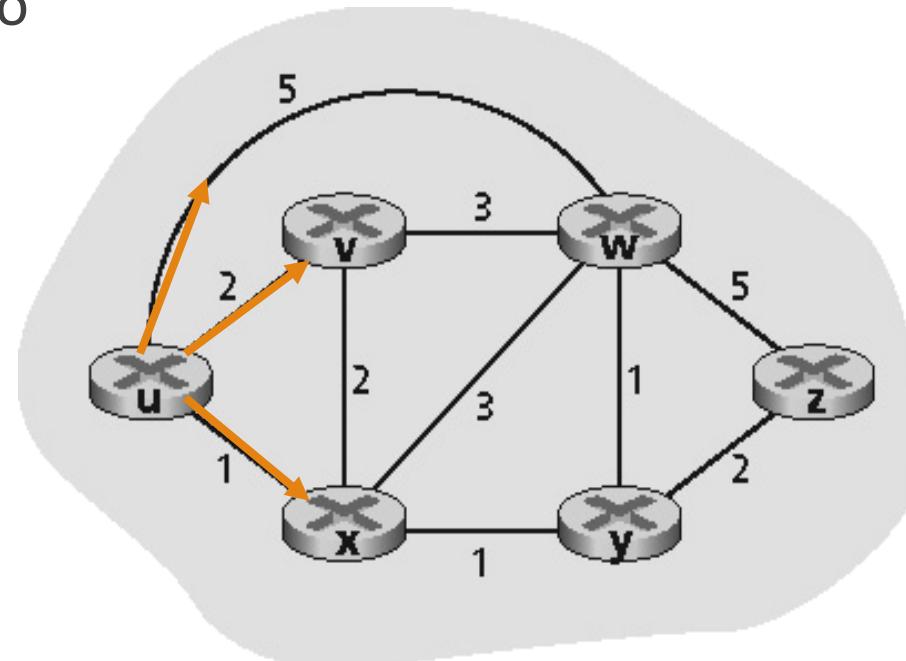
Desvantagem

- Usa mais memória

OSPF: Open Shortest Path First

Fornece balanceamento de carga

- Se o gerenciador especificar várias rotas para determinado destino ao mesmo custo
 - OSPF distribui o tráfego por todas as rotas igualmente
 - RIP calcula uma rota por destino



OSPF: Open Shortest Path First

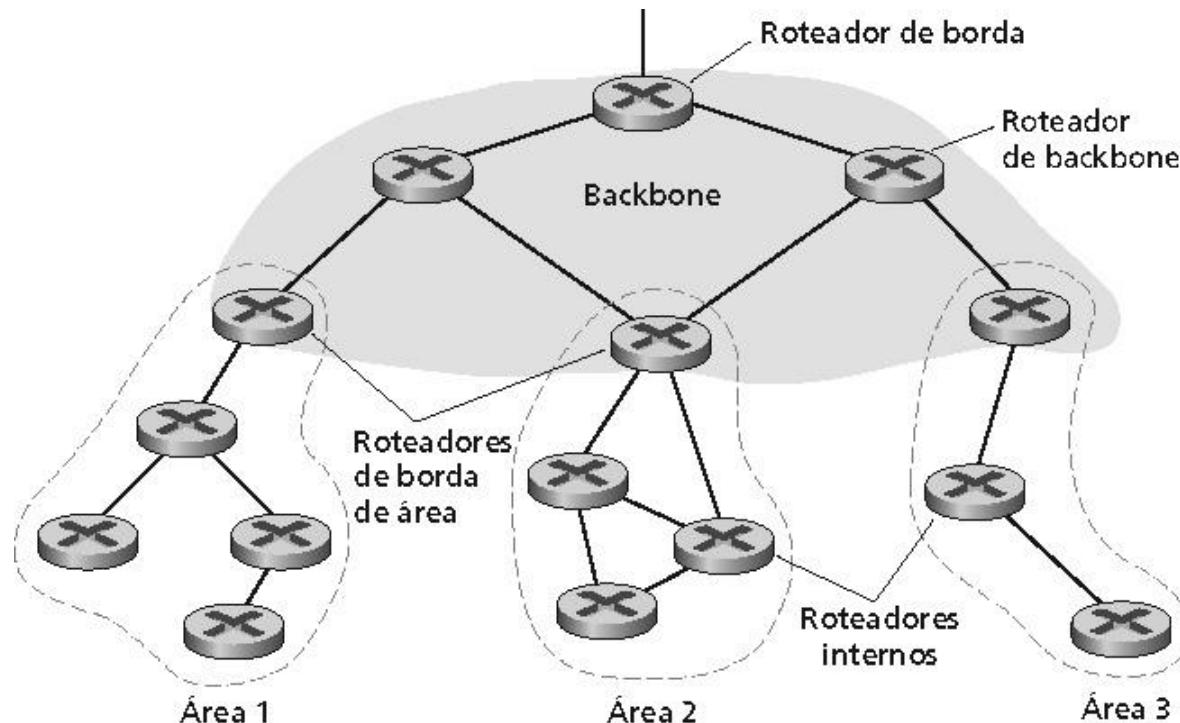
Permite que um domínio particione suas redes e roteadores em subconjuntos chamados de áreas

- Permite o crescimento e faz com que as redes sejam fáceis de gerenciar

OSPF Hierarquia

Hierarquia de dois nível: local area, backbone.

- Avisos de estado dos links apenas na área
- Cada nó conhece a topologia da área; apenas conhece a direção (caminho mais curto) para as outras áreas



OSPF Hierarquia

Roteadores na borda da área

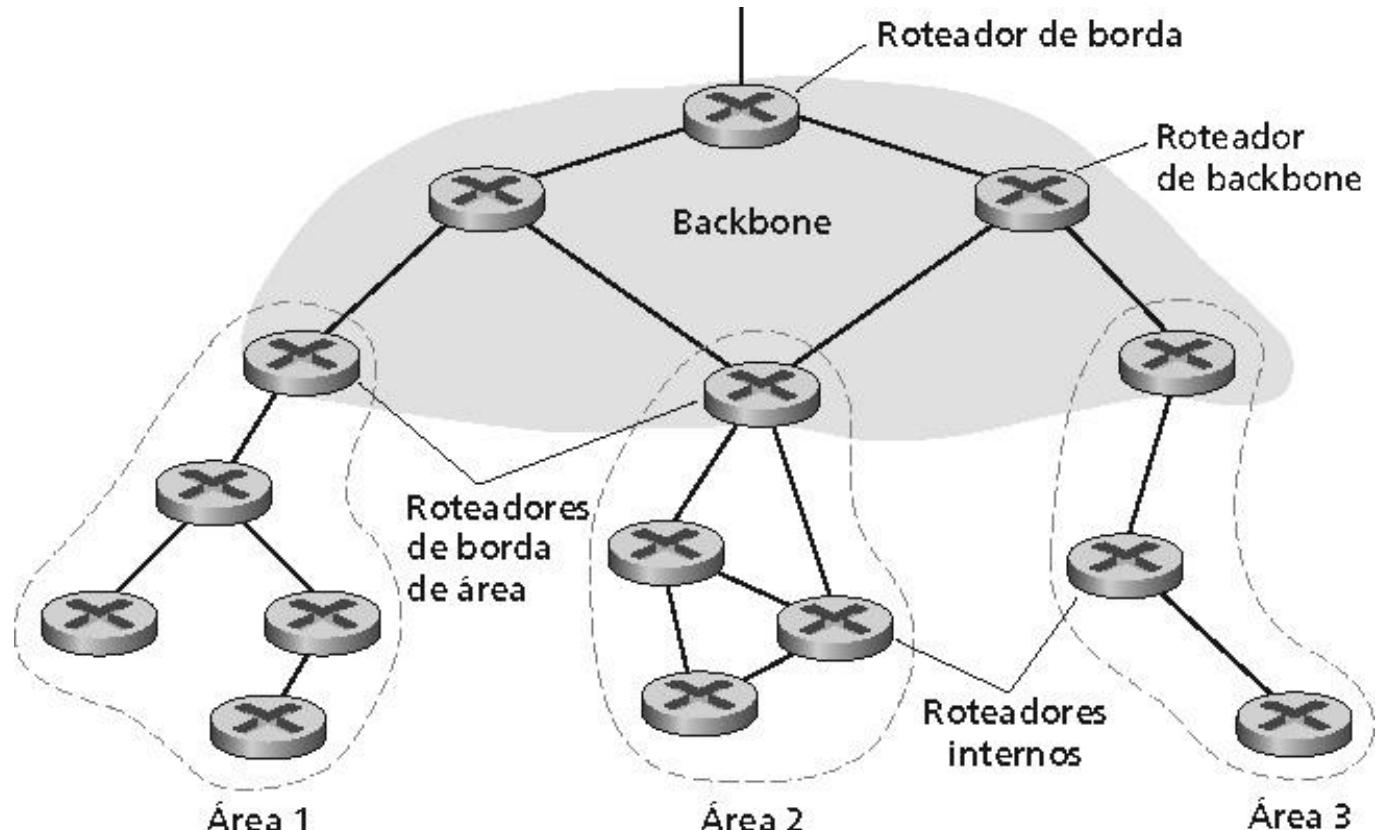
- “resumem” distâncias para redes na sua própria área, avisa outros roteadores de borda

Roteadores Backbone:

- executam o roteamento OSPF limitado no backbone

Roteadores fronteira:

- conecta a outras ASs.



Pontos Importantes

Protocolos de Roteamento RIP e OSPF

- Entender princípios gerais
- Saber comparar os dois protocolos

CAP 6. CAMADA DE REDE

AULA 11: ROTEAMENTO HIERÁRQUICO E O PROTOCOLO BGP

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

Roteamento hierárquico

Nosso estudo até aqui foi uma idealização

- Roteadores são todos idênticos (executam o mesmo algoritmo de roteamento)
- ... na prática, isso não é verdade

Na prática existem mais problemas

- Escala: com mais de 200 milhões de destinos:
 - Não é possível armazenar todos os destinos numa única tabela de rotas!
 - As mudanças na tabela de rotas iriam congestionar os enlaces!
- Autonomia administrativa
 - Internet = rede de redes
 - Cada administração de rede pode querer controlar o roteamento na sua própria rede

Roteamento hierárquico

Agrega roteadores em regiões: “Sistemas Autônomos” (AS)

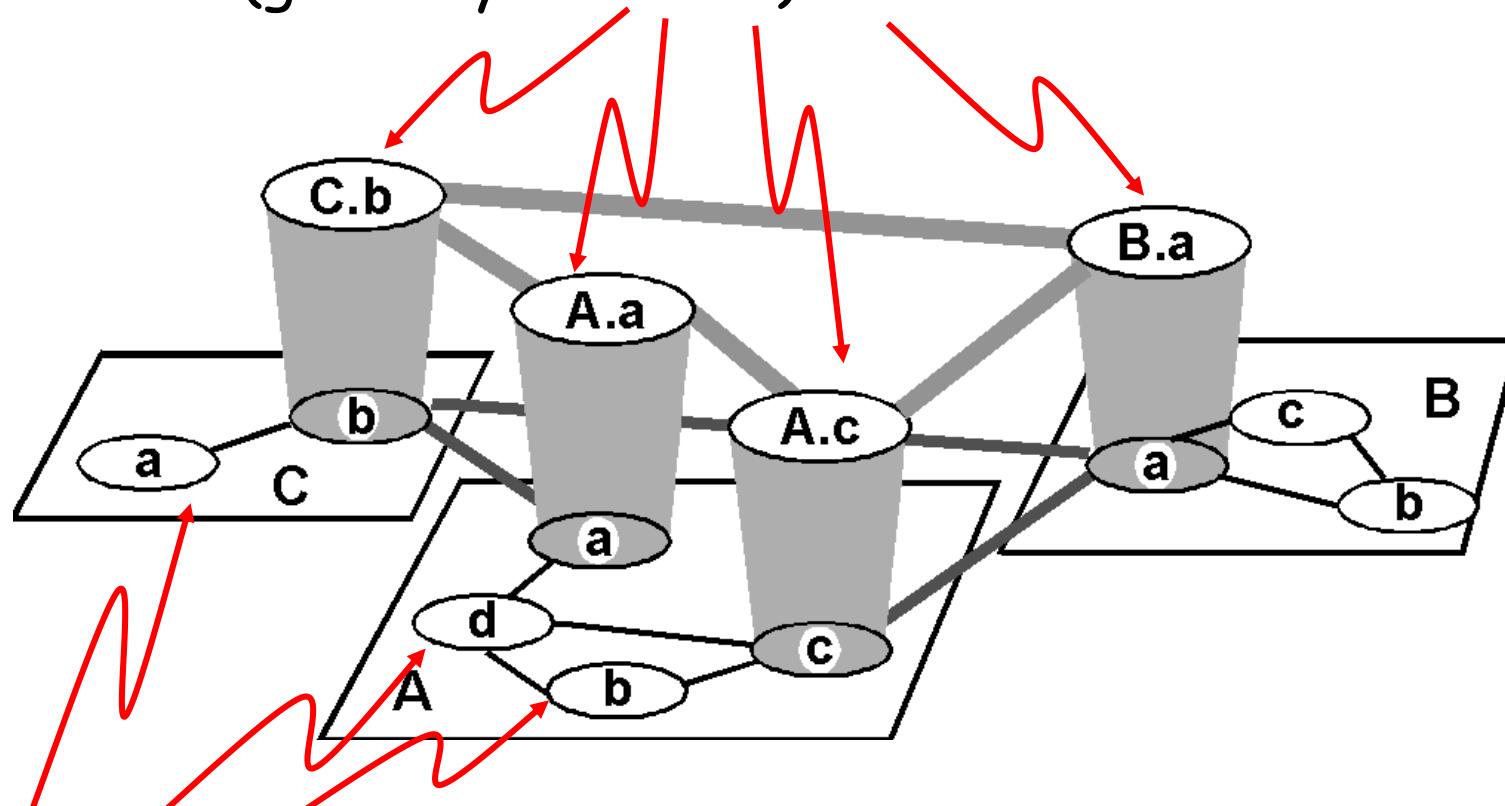
- Roteadores no mesmo AS rodam o mesmo protocolo de roteamento
 - Protocolo de roteamento “intra-AS”
- Roteadores em diferentes AS podem rodar diferentes protocolos de roteamento
- AS são identificadas por ASNs (AS Numbers)
 - <http://www.iana.org/assignments/as-numbers/as-numbers.xhtml>
 - <http://lacnic.net/cgi-bin/lacnic/whois?lg=EN>
 - AS28573 é Claro S.A., AS263300 é UFSC

Roteador de Borda (Gateway)

- Link direto para um roteador em outro AS
- Protocolo de roteamento “inter-AS”

Internet como Hierarquia

Roteador (gateway exterior) Inter-AS

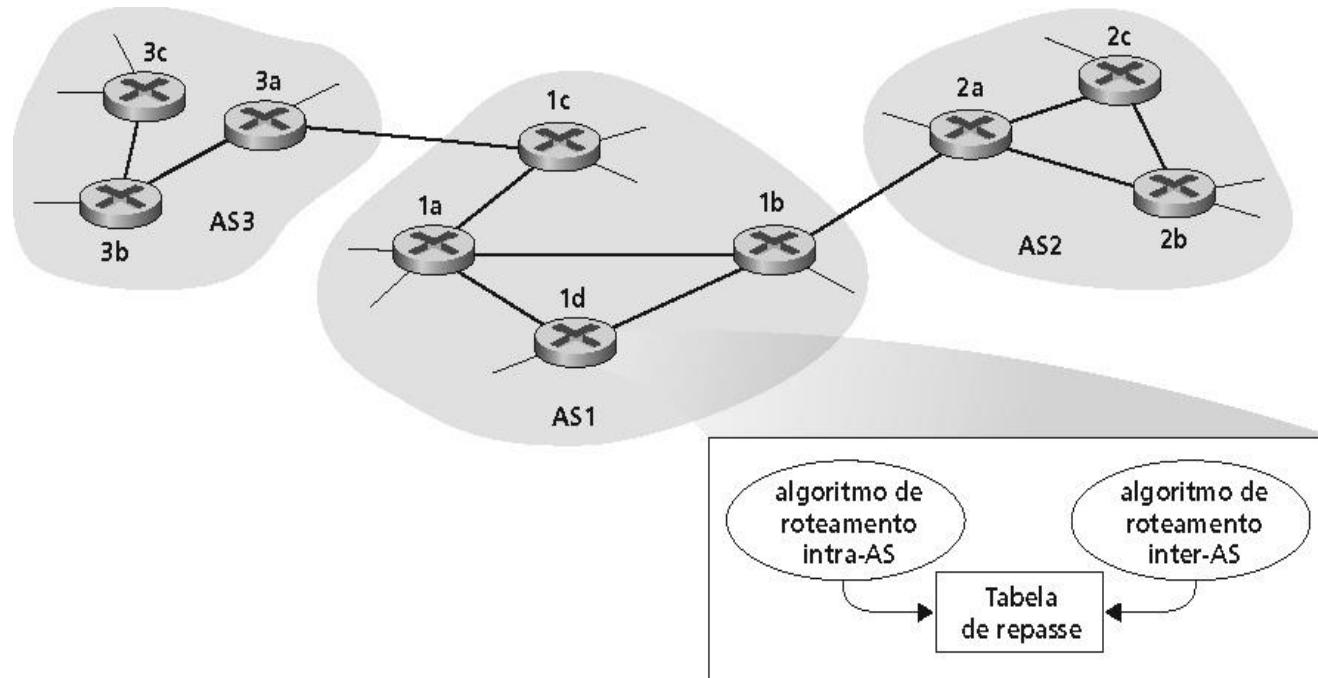


Roteador (gateway interior) Intra-AS

ASs interconectadas

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

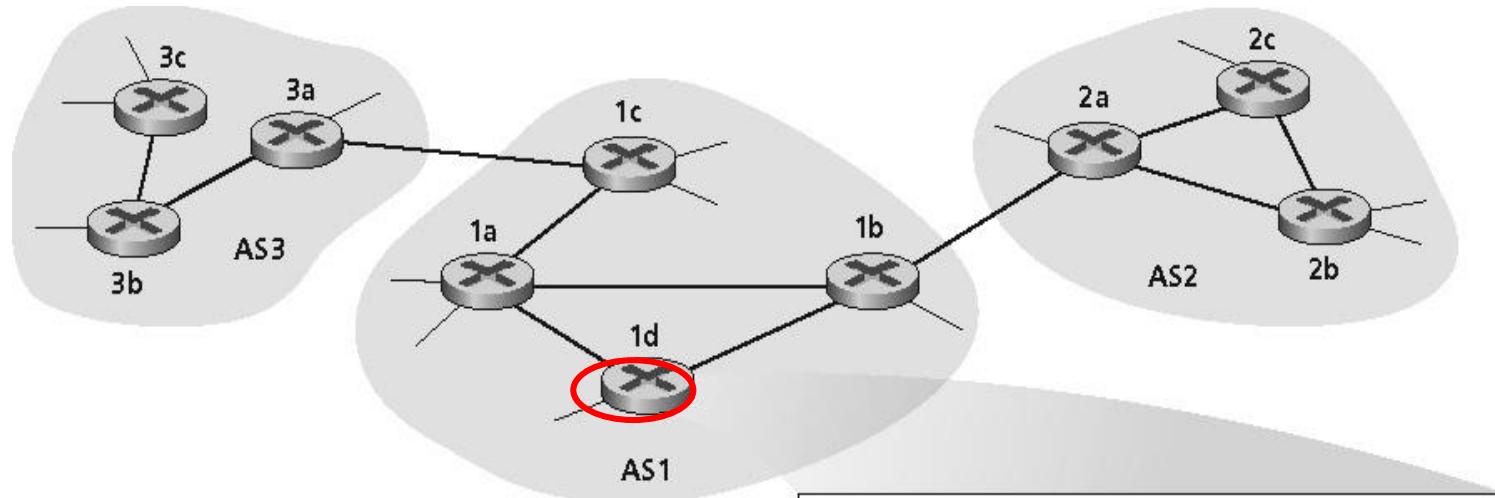
- Intra-AS estabelece entradas na tabela de roteamento para destinos internos
- Inter-AS e intra-AS estabelecem entradas na tabela para destinos externos



Tarefas Inter-AS

Suponha que o roteador 1d no AS1 receba um datagrama cujo destino seja fora do AS1

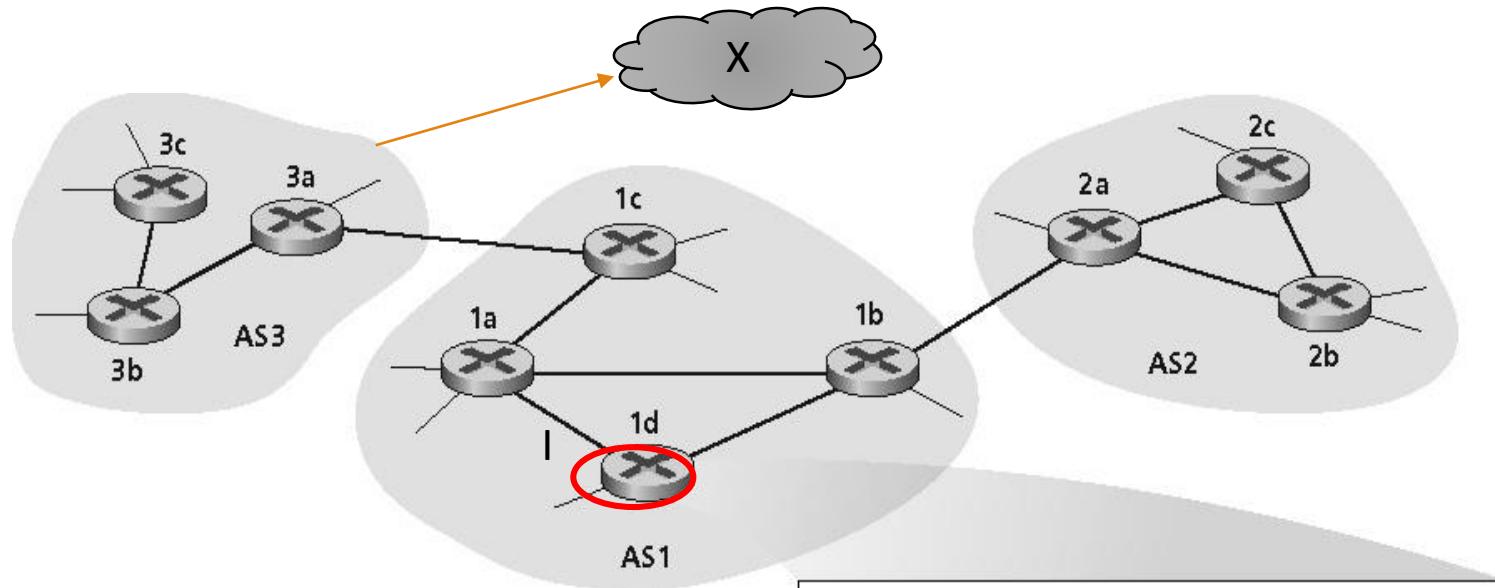
- O roteador deveria encaminhar o pacote para os roteadores de borda, mas qual deles?
- AS1 precisa:
 - 1. Aprender quais destinos são alcançáveis através de AS2 e através de AS3.
 - 2. Propagar suas informações de alcance para todos os roteadores em AS1.
- Tarefa para o roteamento inter-AS!



Tarefas Inter-AS

Exemplo: Ajustando a tabela de roteamento no roteador 1d

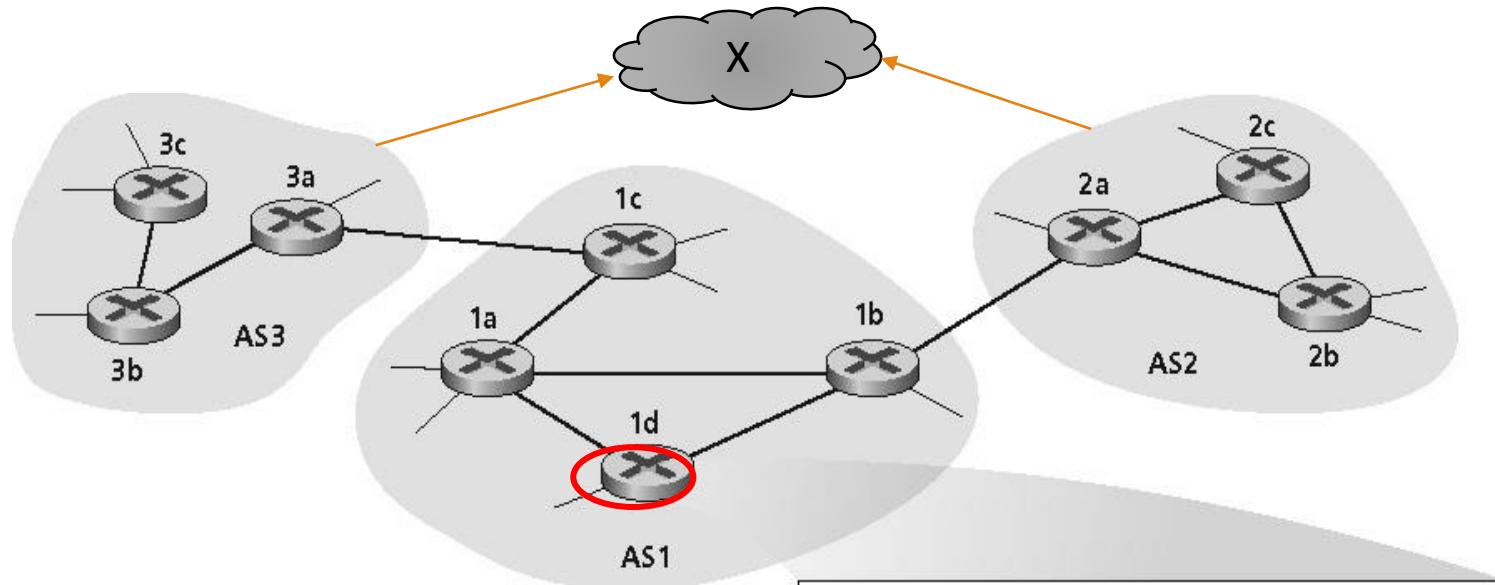
- Suponha que AS1 aprende pelo protocolo inter-AS que a sub-rede x é alcancável através de AS3 (gateway 1c) mas não através de AS2
- O protocolo inter-AS propaga informações de alcance para todos os roteadores internos
- Baseado nas informações de roteamento intra-AS, o roteador 1d determina que sua interface I está no caminho de menor custo para 1c
- Coloca na tabela de roteamento a entrada (x,I)



Tarefas Inter-AS

Exemplo: Escolhendo entre múltiplas Ass

- Agora suponha que AS1 aprende pelo protocolo inter-AS que a sub-rede x é alcançável através de AS3 e através de AS2.
- Para configurar a tabela de roteamento, o roteador 1d deve determinar por qual gateway ele deve encaminhar os pacotes para o destino x.
- Roteamento de “batata quente”: envia o pacote para o mais próximo de dois roteadores
 - Para o roteador com o caminho de menor custo na AS1 (via informações do protocolo intra-AS)



Roteamento na Internet: Intra-AS

Também conhecidos como IGP (Interior Gateway Protocols)

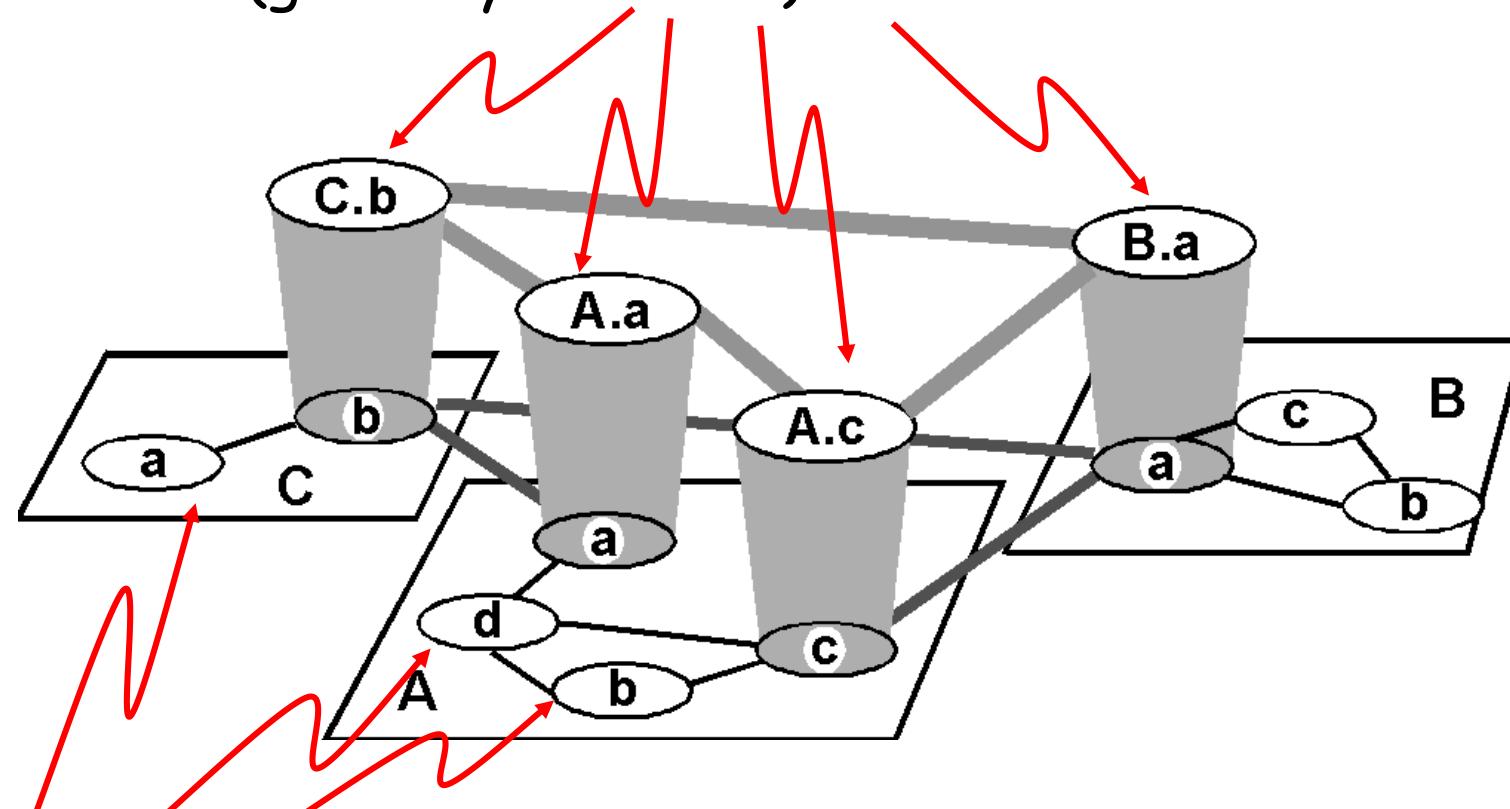
- atuam dentro de um único domínio de roteamento, um único Autonomous System (AS)

IGPs comuns:

- RIP: Routing Information Protocol: Distance Vector
- OSPF: Open Shortest Path First: Link State
- IGRP: Interior Gateway Routing Protocol (Cisco): Distance Vector
- EIGRP: Enhanced IGRP (Cisco): Distance Vector + Link State
- IS-IS: Integrated Intermediate System - Intermediate System: Link State

Internet como Hierarquia

Roteador (gateway exterior) Inter-AS



Roteador (gateway interior) Intra-AS

Roteamento na Internet: Inter-AS

Também conhecidos como EGP (External Gateway Protocols)

- atuam entre Autonomous System (AS)

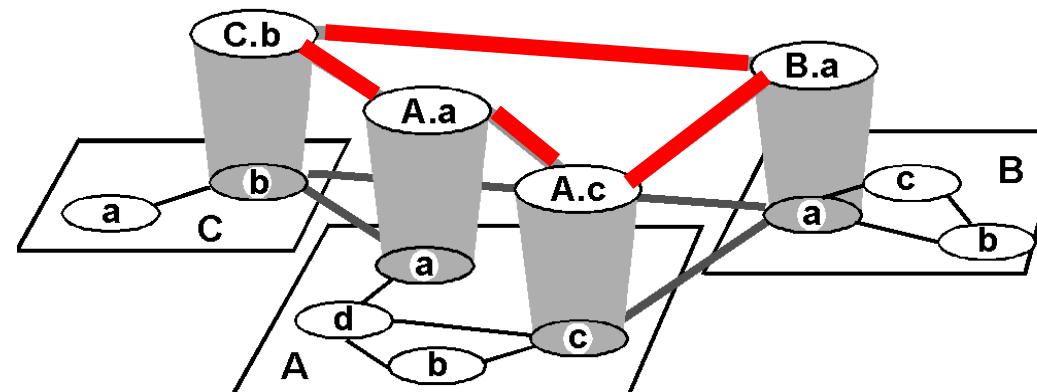
Protocolo único

- BGP-4

Roteamento Internet inter-AS: BGP

BGP (Border Gateway Protocol): é o padrão de fato para uso na Internet

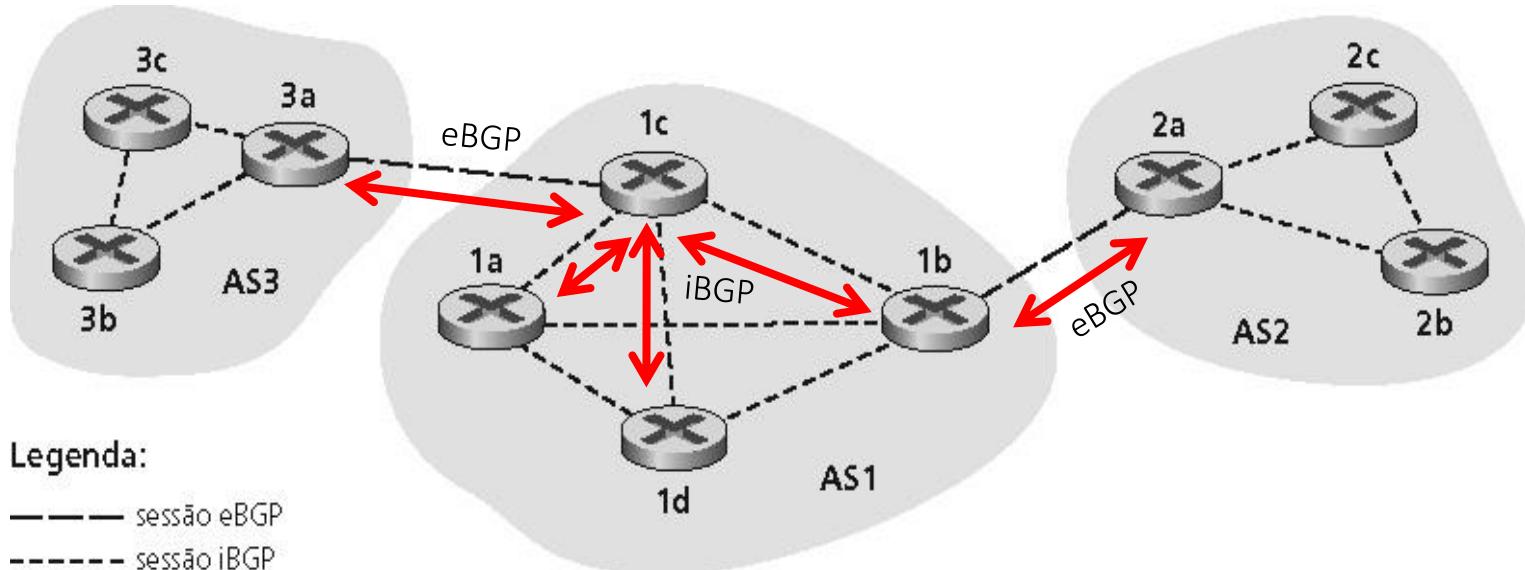
- BGP provê a cada AS meios para:
 - 1. Obter informações de alcance de sub-rede dos ASs vizinhos
 - 2. Propagar informações de alcance para todos os roteadores internos ao AS
 - 3. Determinar “boas” rotas baseado em informações de alcance e política
- Permite que uma subrede comunique sua existência para o resto da Internet: “Estou aqui”



BGP: conceitos básicos

Pares de roteadores (BGP peers)

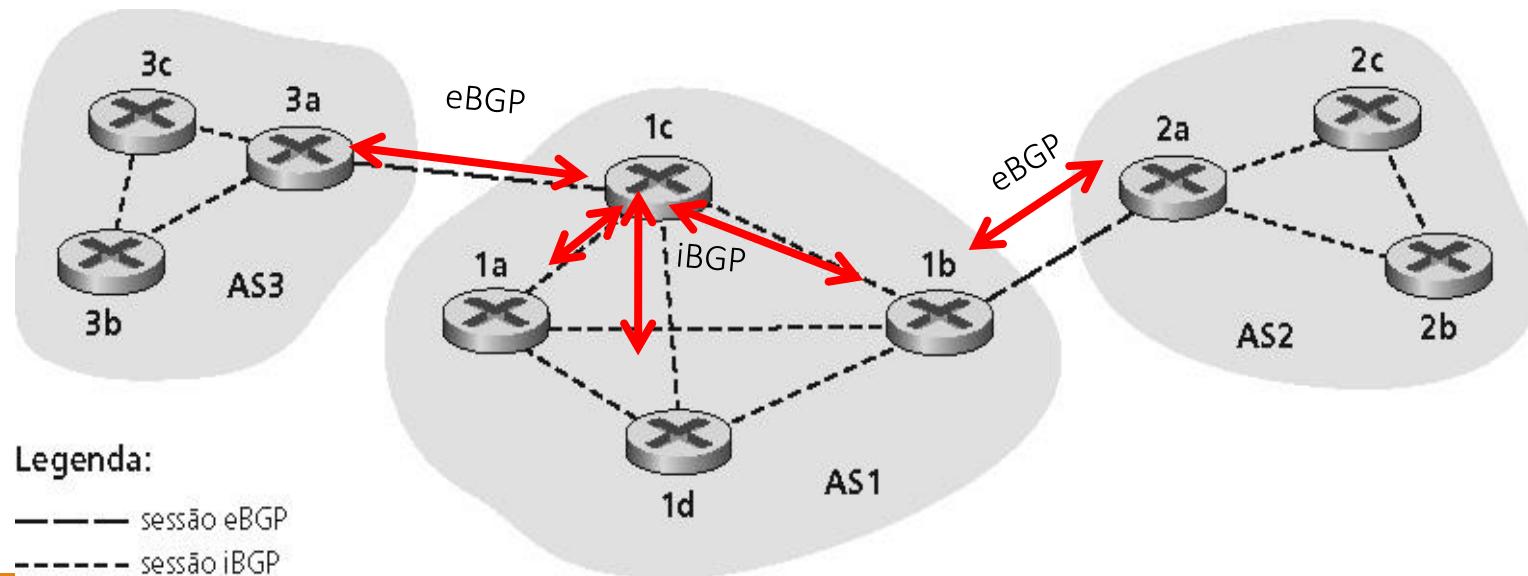
- trocam informações de roteamento por conexões TCP semi-permanentes: sessões BGP
- Quando AS2 comunica um prefixo ao AS1, AS2 está prometendo que encaminhará todos os datagramas destinados a esse prefixo



Distribuindo informações de alcance

Em cada sessão eBGP entre 3a e 1c, AS3 envia informações de alcance de prefixo para AS1

- 1c pode então usar iBGP para distribuir essa nova informação de alcance de prefixo para todos os roteadores em AS1
- 1b pode recomunicar essa nova informação para AS2 por meio da sessão eBGP 1b-para-2a.
- Quando um roteador aprende um novo prefixo, ele cria uma entrada para o prefixo em sua tabela de roteamento.



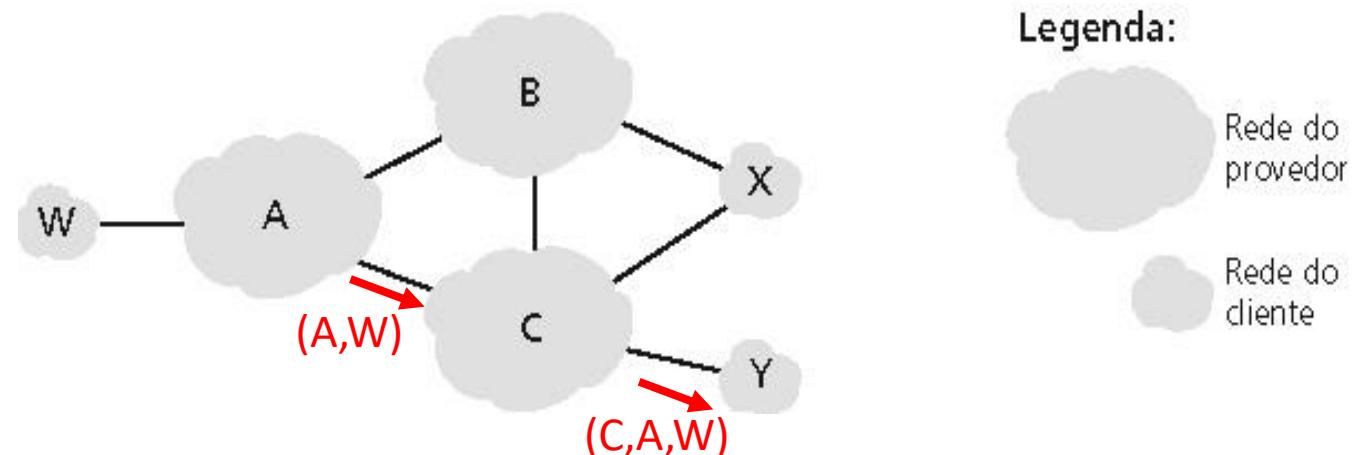
Roteamento Internet inter-AS: BGP

Protocolo Path Vector

- Similar ao protocolo Distance Vector
- Cada Border Gateway difunde para seus vizinhos (pares) o caminho completo (sequência de ASs) para o destino: AS-PATH
- contém os ASs (AS number) pelos quais o comunicado para o prefixo passou: AS 67 - AS 17 - ...

Quando um roteador gateway recebe um comunicado de rota

- ele usa política de importação para aceitar/rejeitar.

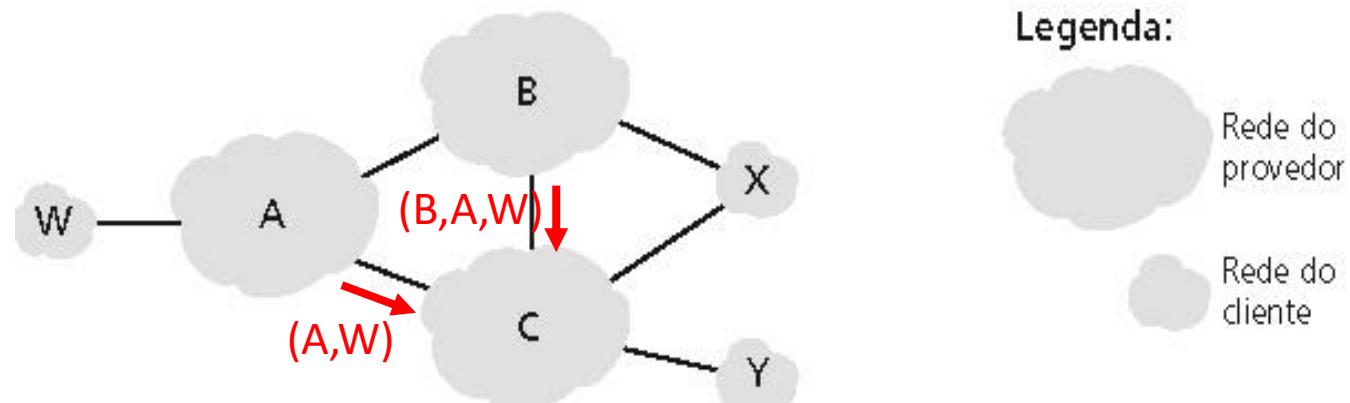


BGP: seleção de rota

Um roteador pode aprender mais de uma rota para o mesmo prefixo. O roteador deve selecionar uma rota

Regras de eliminação:

- Decisão de política
- AS-PATH (caminho) mais curto
- Roteamento da “batata quente”



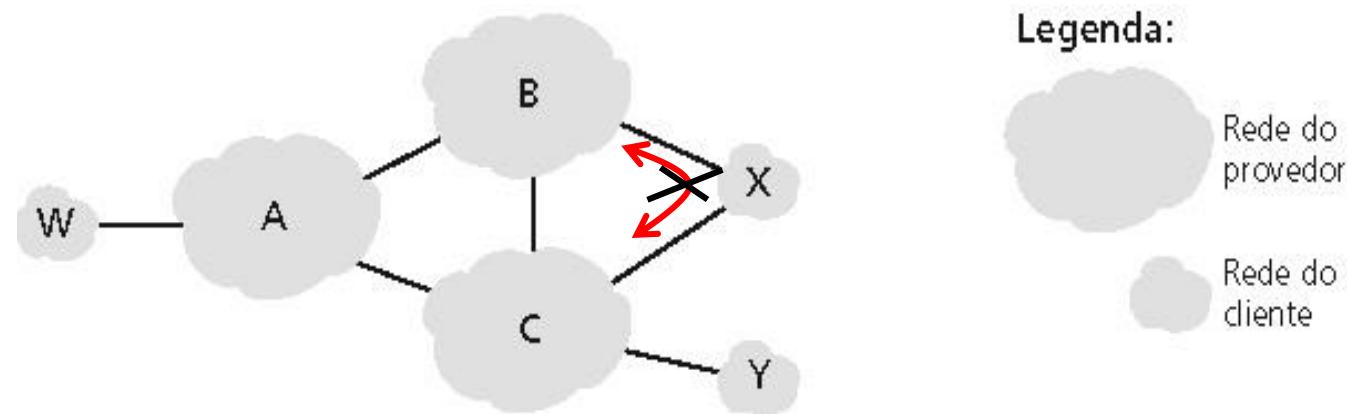
BGP: política de roteamento

Legenda

- A, B, C são redes de provedores
- X, W, Y são clientes (das redes dos provedores)

X é dual-homed: anexados a duas redes

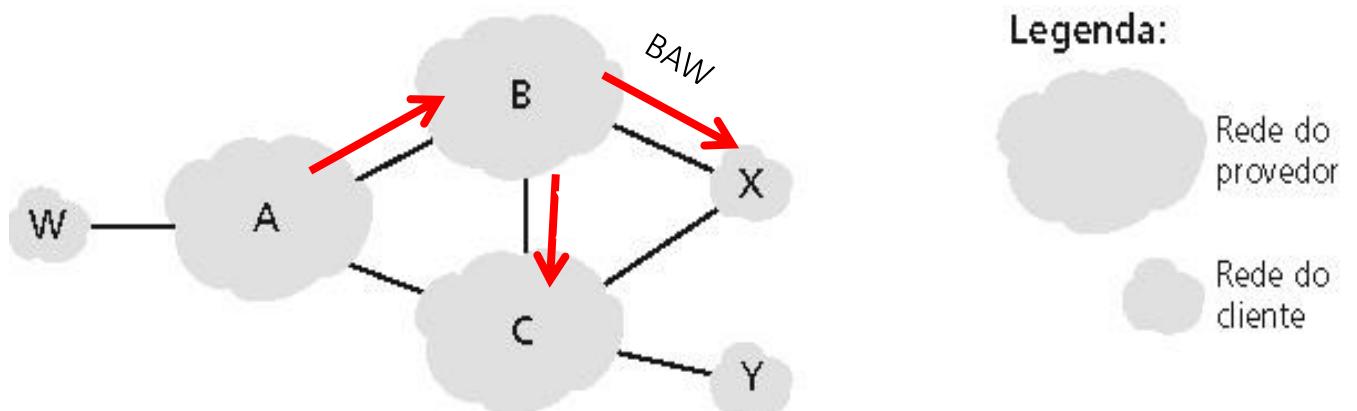
- X não quer rotear de B para C
- ... então X não comunicará ao B uma rota para C



BGP: política de roteamento (2)

Anúncios

- A comunica ao B o caminho AW
- B comunica ao X o caminho BAW
- B deveria comunicar ao C o caminho BAW?
- De jeito nenhum! B não obtém nenhum “rendimento” em rotear CBAW pois nem W nem C são seus clientes
- B quer rotear somente de/para seus clientes!
- B quer forçar C a rotear para W via A
- Não anuncia esta rota



Porque protocolos Intra- e Inter-AS são diferentes ?

Políticas:

- 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: as decisões políticas são mais simples

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 podem ser mais importantes que desempenho

Pontos Importantes

Roteamento Hierárquico e BGP

- Entender princípios gerais
- Porque existem protocolos intra e inter-AS

CAP 6. CAMADA DE REDE

AULA 12: IPV6 – MOTIVOS DA SUBSTITUIÇÃO DO IPV4

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://MOODLE.UFSC.BR)

Uma “nova versão” do protocolo Internet IP

- IETF decidiu desenvolver uma nova versão do IP pois o espaço de endereçamento disponível do IPv4 provavelmente terminaria no início do século 21
- RFC 2460 (Dezembro de 1998), RFC8200 (2017) tornou Internet Standard
- Baseado nos principais paradigmas IPv4
 - sem conexão, sem controle de erro e de fluxo na camada de rede
- Projetado para ser um passo evolucionário do IPv4
 - Aumento do espaço de endereçamento, autenticação e criptografia
 - Extensões para fluxos de dados multimídia
 - Mais suporte à mobilidade

Compatível com IPv4

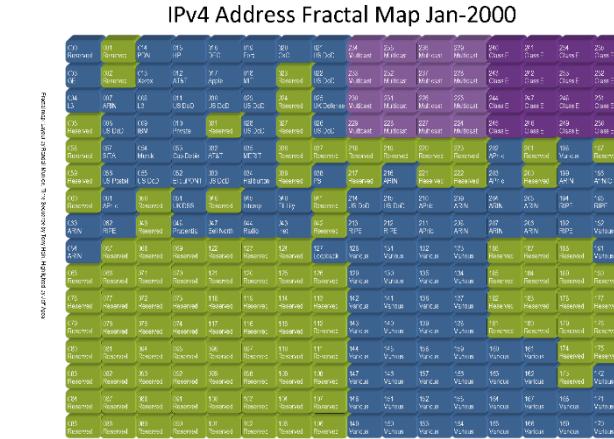
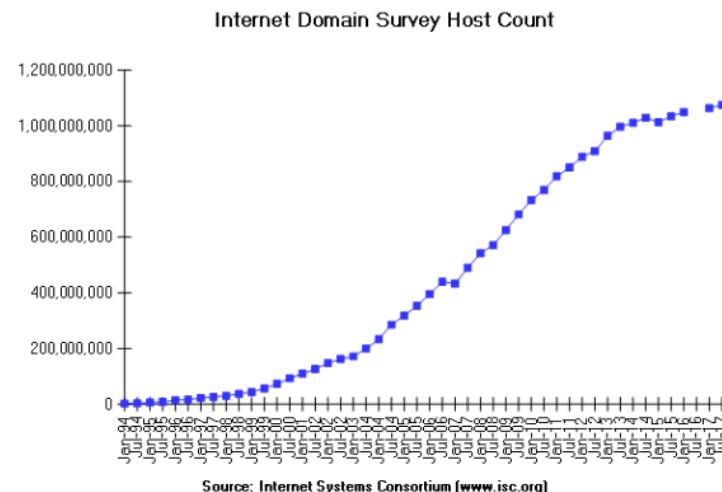
- Uma importante meta de projeto do IPv6 é a compatibilidade com IPv4
 - novos hosts e roteadores executando IPv6 são capazes de coexistir com hosts IPv4
 - habilitando assim uma migração gradativa da Internet

Motivos que levam à substituição do IPv4

O espaço de endereçamento do IPv4 é insuficiente (32 bits)

- $2^{32} = 4.294.967.296$
(4 bilhões de endereços)
- Menos vários endereços não utilizados

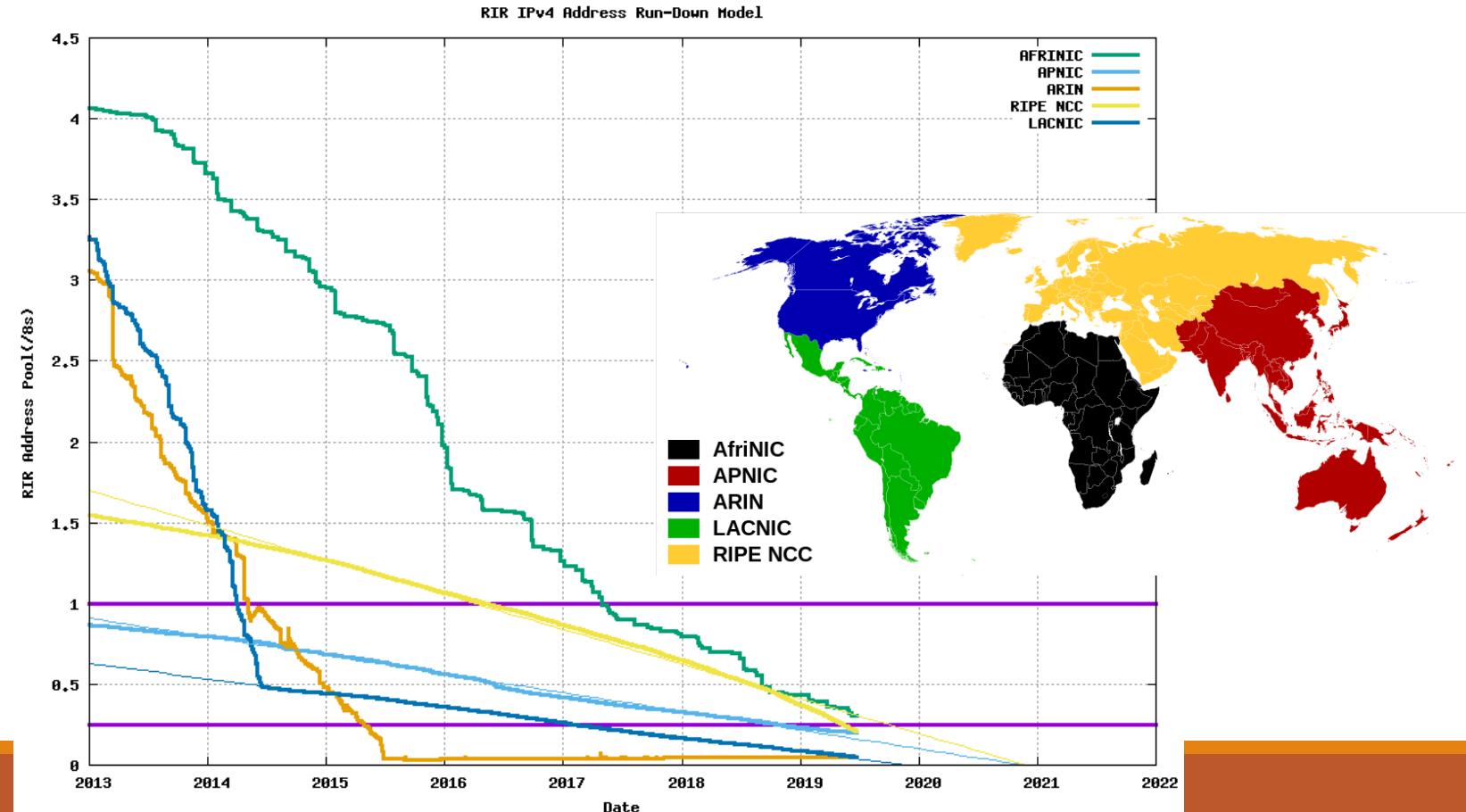
O crescimento da Internet é exponencial



Motivos que levam à substituição do IPv4

O espaço de endereçamento do IPv4 é insuficiente (32 bits)

- Estoque IANA esgotou em 31/01/2011
- E os estoques das RIRs estão no final



Motivos que levam à substituição do IPv4

Medidas Paliativas: CIDR

- A política de alocação inicial não foi favorável a uma utilização racional dos mesmos. Dividiu-se esse espaço em 3 classes:
 - Classe A: com 128 segmentos atribuídos individualmente às entidades que deles necessitassem, com 16 milhões de endereços cada. Ela utilizava o espaço compreendido entre os endereços 00000000.*.*.* (0.*.*.*.) e 01111111.*.*.* (127.*.*.*.).
 - Classe B: com 16 mil segmentos de 64 mil endereços cada. Essa classe era classificada como /16. Ela utilizava o espaço compreendido entre os endereços 10000000.00000000.*.* (128.0.*.*.) e 10111111.11111111.*.* (191.255.*.*.).
 - Classe C: 2 milhões de segmentos de 256 endereços cada. Essa classe era classificada como /24. Ela utilizava o espaço compreendido entre os endereços 11000000.00000000.00000000.* (192.0.0.*.) e 11011111.11111111.11111111.* (213.255.255.*).
- Além disso, 32 blocos /8 restantes foram reservados para Multicast e para a IANA.

Motivos que levam à substituição do IPv4

Medidas Paliativas: CIDR

- CIDR (de Classless Inter-Domain Routing) RFC 1519, 1993.
 - Permitindo flexibilidade quando dividindo margens de endereços IP em redes separadas
 - Usa máscaras de comprimento variável - VLSM (de Variable Length Subnet Masks)
 - para alocar endereços IP em subredes de acordo com as necessidades individuais e não nas regras de uso generalizado em toda a rede
 - a divisão de rede/host pode ocorrer em qualquer fronteira de bits no endereço
 - Promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos.

Motivos que levam à substituição do IPv4

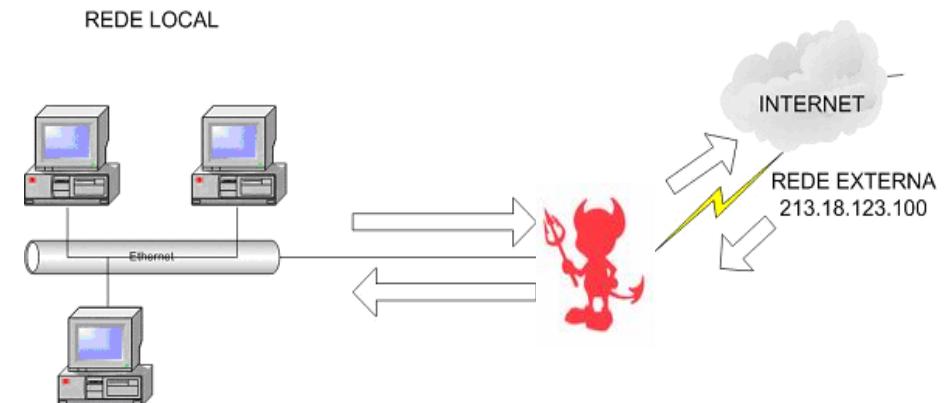
Medidas Paliativas:

- RFC 1918 (endereços privados)
 - Permite o uso de endereços não válidos na Internet nas redes corporativas
- NAT (tradução de endereços)
 - Permite que com um endereço válido na Internet apenas, toda uma rede de computadores usando endereços privados seja conectada (mas com restrições)
- DHCP (alocação dinâmica de endereços IP)
 - Permite que provedores reutilizem endereços Internet para conexões não permanentes

Motivos que levam à substituição do IPv4

Medidas Paliativas:

- ... mas também colaborando para a demora em sua adoção!
- Alguns questionam porque não utilizar o NAT indefinidamente, mas ele foi concebido como uma solução provisória!
- O NAT acaba com o modelo de funcionamento fim a fim, trazendo complicações ou impedindo o funcionamento de uma série de aplicações.
- O NAT tem alguns problemas técnicos:
 - Não é fácil manter o estado do NAT no caso de falha em um dos hosts.
 - O NAT não funciona bem com o IPsec.
 - O NAT não escala bem



A razão principal para o IPv6 é, então...

A necessidade de mais endereços Internet!

- Para suportar seu crescimento:
 - Possibilitando a interligação de mais redes, de forma que a expansão da economia, com novas empresas, novos negócios seja suportada.
 - A fim de que todos possam ser incluídos digitalmente, em especial nos países em desenvolvimento
 - Com o uso de novas aplicações, como sua utilização em dispositivos móveis com tecnologia 4G/5G, por exemplo, ou em eletrodomésticos e outros aparelhos com eletrônica embarcada
 - Com a eliminação de tecnologias como o NAT, que dificultam o funcionamento de várias aplicações

A razão principal para o IPv6 é, então...

Um endereço IPv4 é formado por 32 bits.

- $2^{32} = 4.294.967.296$ endereços aproximadamente 4 bilhões de endereços
- Muitos endereços são reservados

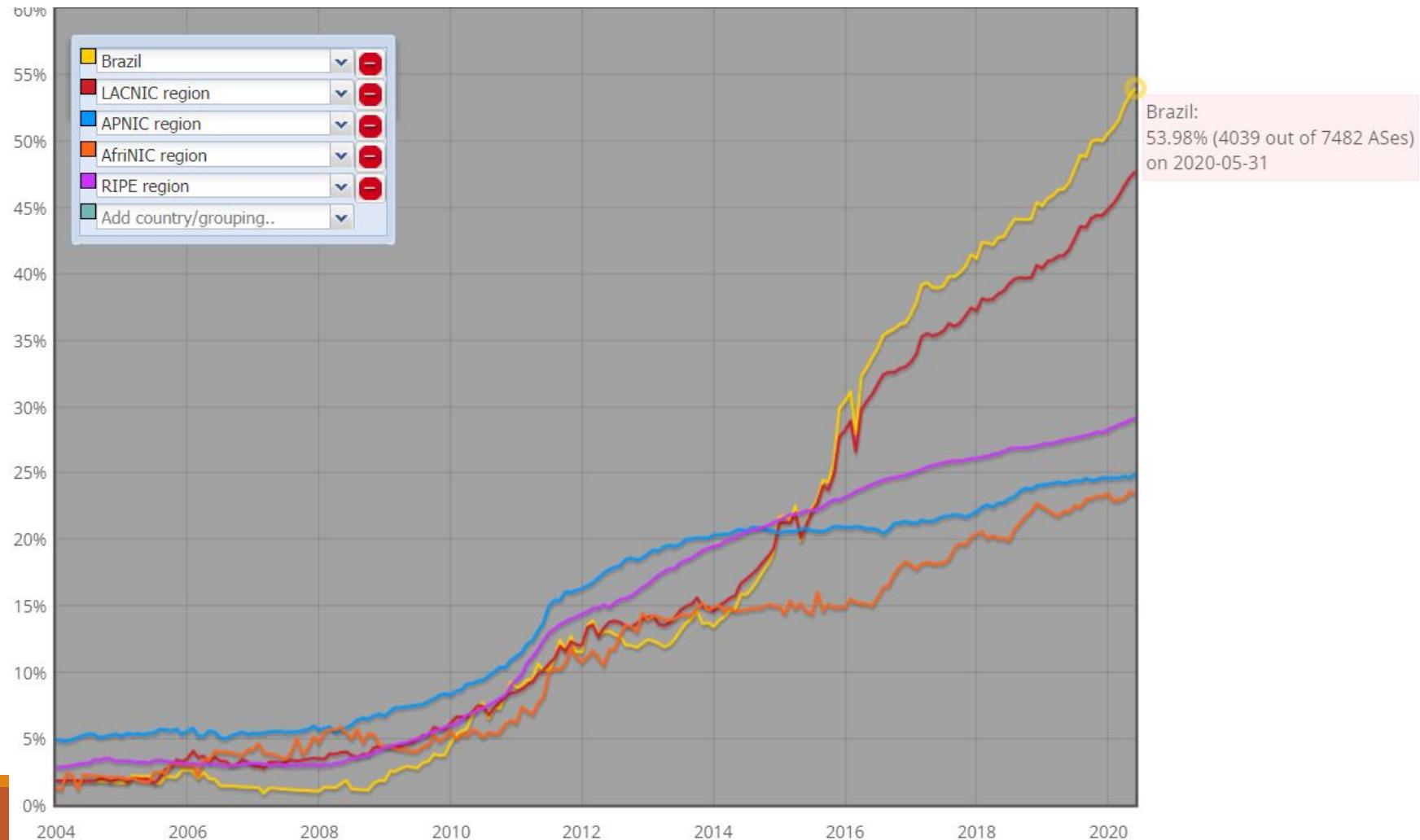
Um endereço IPv6 é formado por 128 bits.

- $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ endereços
- ~ 79 trilhões de trilhões de vezes mais que no IPv4.
- ~ 5.6×10^{28} endereços IP por ser humano.
- Distribuídos na terra: $665,570,793,348,866,943,898,599/m^2$
- Estimativa pessimista com hierarquias: ~1,564 endereço/ m^2

IPv6 está sendo adotado!

<http://v6asns.ripe.net/v/6>, <https://www.pop-sc.rnp.br/monitoramento/ipv6/>

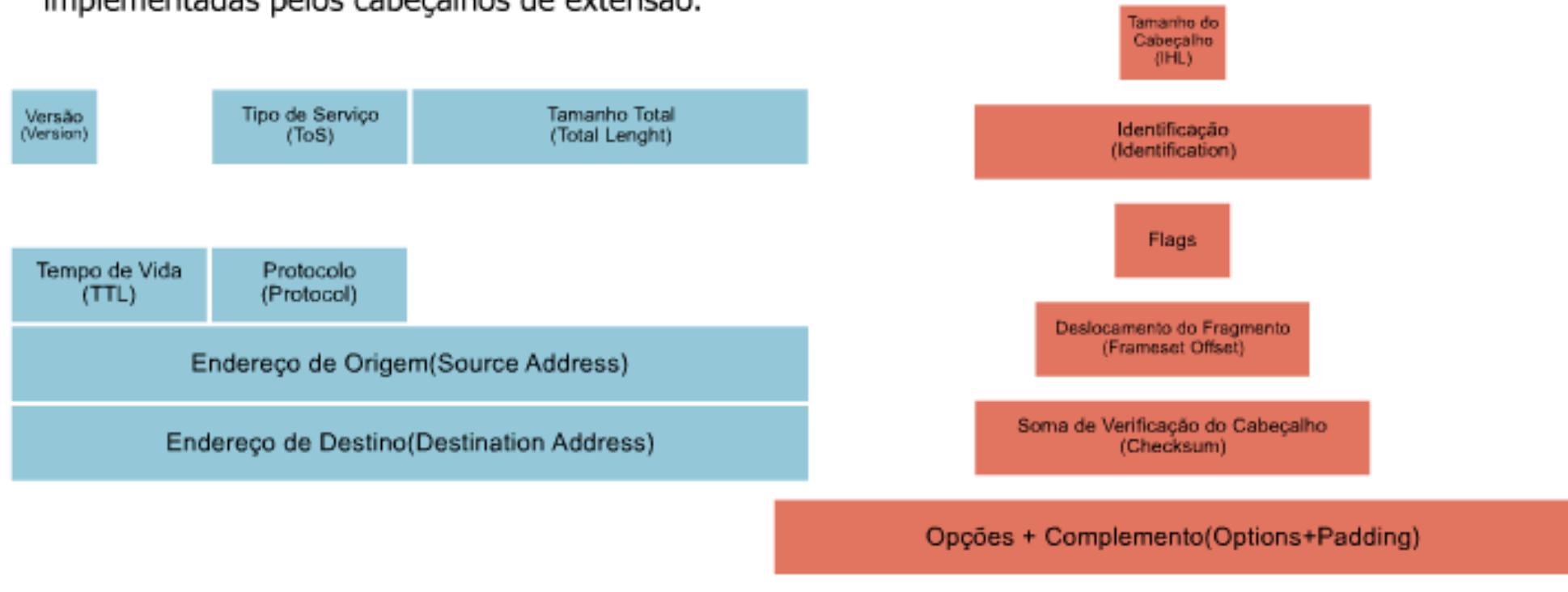
<http://ix.br/trafego/agregado/sp/v6>, <http://ipv6.br/>



Cabeçalho IPv6

Cabeçalho IPv4 => Cabeçalho IPv6

Seis campos do cabeçalho IPv4 foram removidos, pois suas funções não são mais necessárias ou são implementadas pelos cabeçalhos de extensão.



Cabeçalho IPv6

Formato dos cabeçalhos fixos

- Usa cabeçalho de extensão em vez de options

Remove o header checksum

- Confiabilidade da camada de enlace e camadas mais altas para verificar a integridade dos dados

Remove segmentação hop-a-hop

- Sem fragmentação devido a descoberta do MTU do caminho

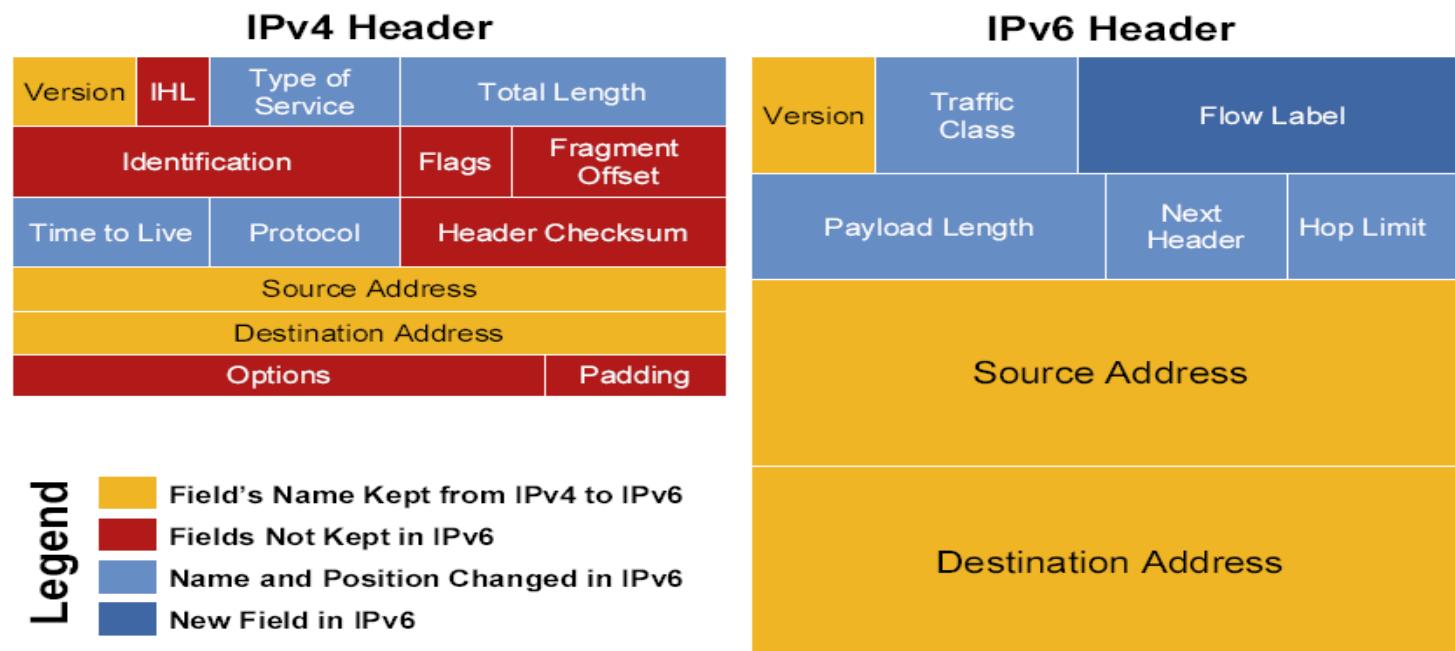
Cabeçalho IPv6

Mais simples

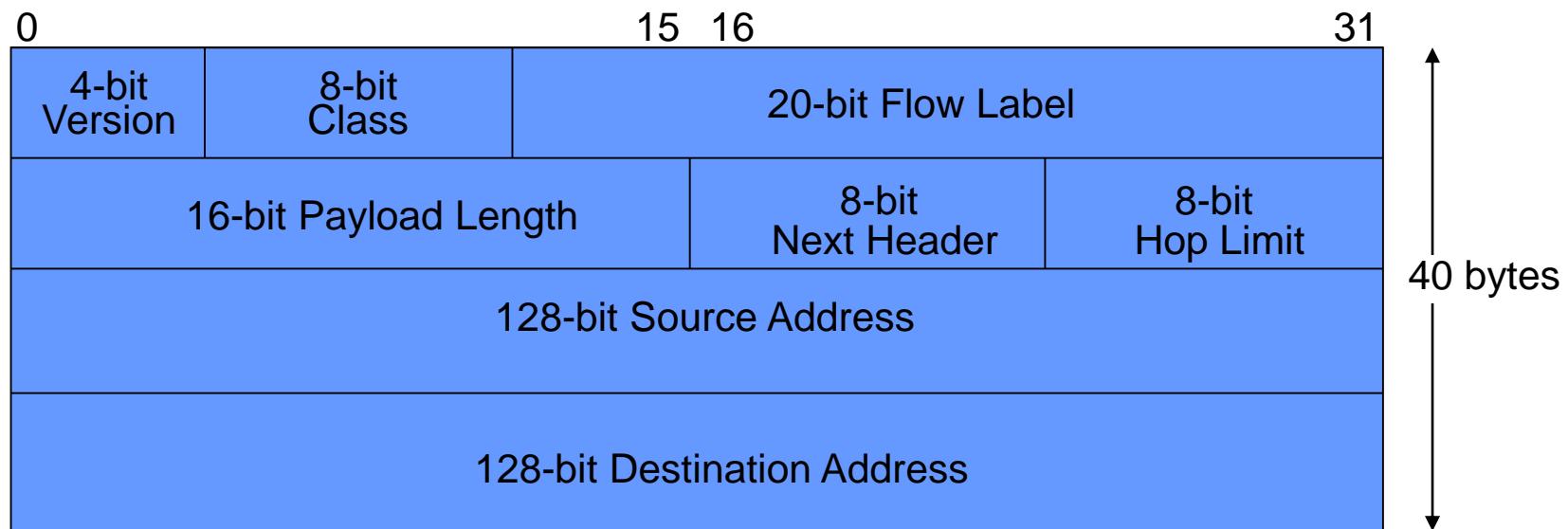
- 8 campos (40 bytes) => IPv4 tem normalmente 20 bytes

Mais flexível

- Prevê sua extensão, através do uso cabeçalhos adicionais



Cabeçalho IPv6



| | |
|----------------|---|
| Version | Único campo idêntico ao IPv4. Código é 6 em IPv6 |
| Class | Facilita manipulação do tráfego tempo real |
| Flow Label | Distingue pacotes requerendo o mesmo tratamento |
| Payload Length | Substitui campo <i>length</i> do IPv4. Dá o tamanho do dado seguindo o cabeçalho IPv6 |
| Next Header | Substitui campo <i>protocol</i> do IPv4. Cabeçalhos de extensão pode ser usado. |
| Hop Limit | Substitui campo <i>TTL</i> do IPv4. Limite de hop reflete melhor o uso. |
| Src Address | 128 bits no IPv6 vs 32 bits no IPv4. |
| Dst Address | 128 bits no IPv6 vs 32 bits no IPv4. |

Formato do cabeçalho IPv6

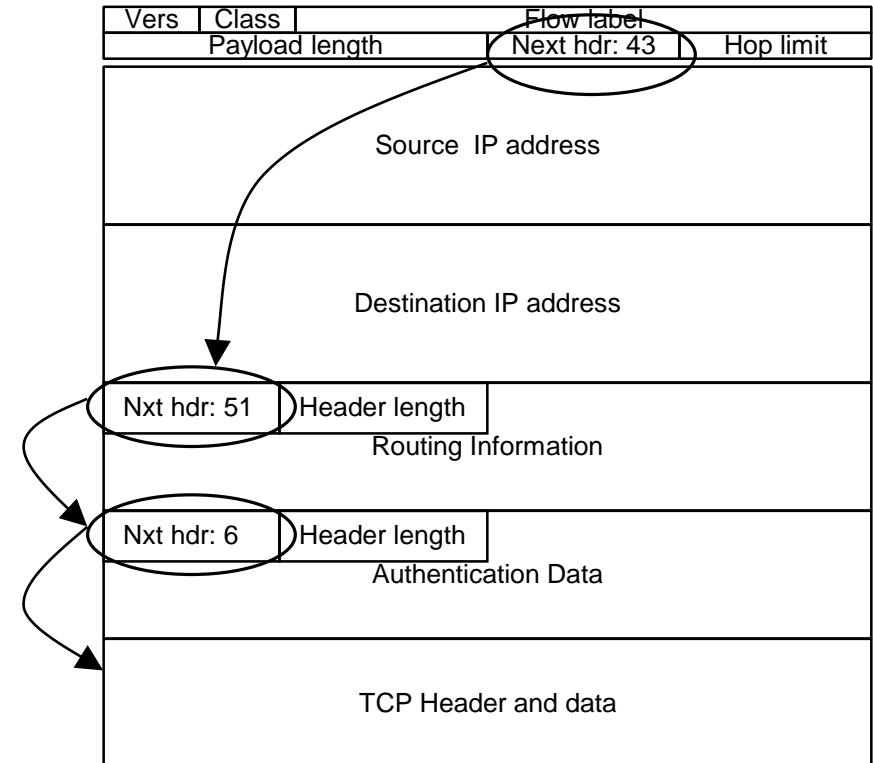
Campo *flow label*

- Permite a identificação de todos os pacotes de um mesmo fluxo de dados
 - fluxo é uma sequência de pacotes enviados por um host para um endereço unicast ou multicast
 - todos os roteadores no caminho podem identificar os pacotes de um fluxo e tratar eles de um modo específico ao fluxo
 - Por exemplo, eles podem escalarizar pacotes de um fluxo de áudio com uma mais alta prioridade que aqueles pertencente a um fluxo de transferência de arquivo

Cabeçalhos de extensão

Dá mais funcionalidade ao IP

- Vários cabeçalhos de extensão do IPv6 são opções no IPv4 (campo option do cabeçalho IPv4)
- Cabeçalhos de extensão são colocados entre o cabeçalho base IPv6 e o cabeçalho do nível de transporte (TCP/UDP)



Cabeçalhos de extensão

Cada cabeçalho tem um tamanho múltiplo de 8 bytes

Os seguintes cabeçalhos já foram definidos:

| Valor | Nome do cabeçalho | Definição |
|-------|--------------------------------|--|
| 0 | Hop-By-Hop | Transporta informações opcionais que são processadas em cada nó ao longo do caminho do pacote, incluindo a origem e o destino. |
| 60 | Destination Options | Transporta informações opcionais que são processadas apenas pelo destino final do pacote. |
| 43 | Routing | Utilizado no suporte a mobilidade do IPv6, ele armazena o endereço original de um nó móvel (Type 2). |
| 44 | Fragmentation | Utilizado pela origem para enviar pacotes maiores do que a Maximum Transmit Unit (MTU) de um caminho. Ao contrário do IPv4, a fragmentação no IPv6 não ocorre nos roteadores encontrados ao longo do caminho do pacote, apenas na origem, sendo re-agrupados no destino final. |
| 51 | Authentication | Utilizado pelo serviço IPSec (IP Security) para prover autenticação e garantia de integridade aos pacotes IPv6. Esse cabeçalho é idêntico ao utilizado no IPv4. |
| 50 | Encapsulating Security Payload | Também utilizado pelo IPSec, provê integridade e confidencialidade para os pacotes. |

Endereços IPv6

Notação decimal em coluna com oito inteiros hexadecimais de 16 bits

- 68E8:1480:0022:0000:ABC1:0000:0000:01FE

Zeros podem ser resumidos

- 68E8:1480:22:0:ABC1:0:0:1FE

Compressão de zeros: zeros podem ser substituído por “::”

- 68E8:1480:22:0:ABC1:0:0:1FE substituído por 68E8:1480:22:0:ABC1::1FE
- Só pode ser realizada uma única vez, caso contrário poderia haver ambiguidade:
 - 2001:0000:0000:0058:0000:0000:0000:0320 poderia ser anotado:
 - 2001::58:0:0:320 ou 2001:0:0:58::320
 - Mas nunca 2001::58::320

Endereços IPv6

Endereço de Rede

- Similar ao IPv4: parte de host é 0
- Exemplo: endereço de sub-rede 2001:0000:0004:CFE, possui 60 bits de prefixo pode ser representado das seguintes formas:
 - 2001:0000:0004:CFE0:0000:0000:0000:0000/60
 - Retirando os zeros a esquerda: 2001:0:4:CFE0:0:0:0:0/60
 - Abreviando: 2001:0:4:CFE0::/60

Endereços IPv6

Alguns prefixos alocados

| Alocação | Prefixo (Binário) |
|---|-------------------|
| Reservado | 0000 0000 |
| Reservado para Alocação NSAP (Network Service Access Point address) | 0000 001 |
| Reservado para Alocação IPX (Internetwork Packet Exchange) | 0000 010 |
| Aggregatable Global Unicast Address | 001 |
| Site-local Unicast Address | 1111 1110 10 |
| Link -local Unicast Address | 1111 1110 11 |
| Multicast Address | 1111 1111 |

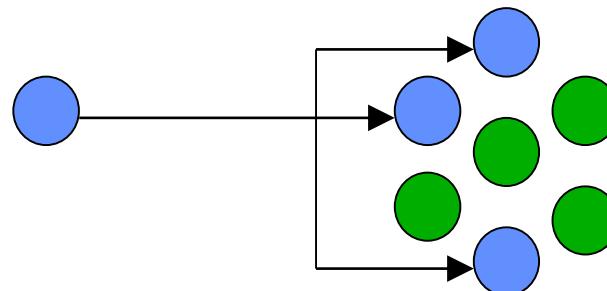
Endereços IPv6

IPv6 tem três categorias de endereçamento:

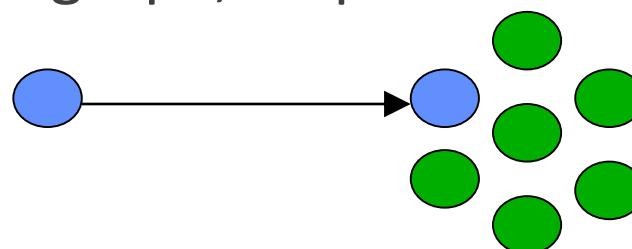
- unicast – identifica uma interface



- multicast – identifica um grupo; pacote é transmitido para todos os membros do grupo



- anycast – identifica um grupo; pacote normalmente é transmitido ao membro mais próximo do grupo, respeitando os critérios de roteamento



Endereços IPv6 Unicast

Identifica apenas uma única interface

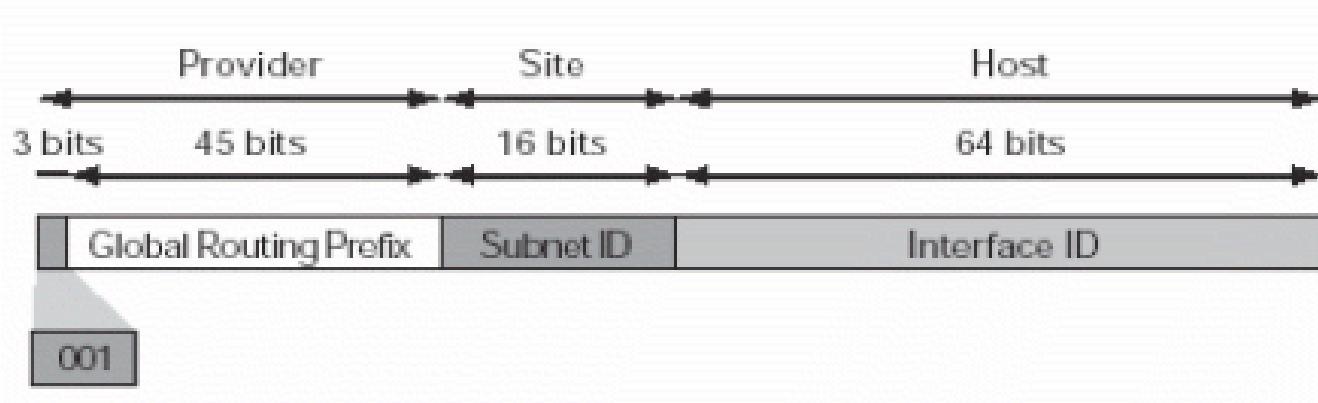
Foram definidos pela RFC 2374 vários tipos de endereços Unicast :

- Aggregatable Global Unicast Address
- Loopback Address (::1)
- Unspecified Address (::)
- NSAP Address: suporte para endereçamento OSI NSAP (prefixo 0000001)
- IPX Address (prefixo 0000010)
- Site-local Unicast Address
- Link-local Unicast Address
- IPv4-compatible IPv6 Address (::172.16.1.2)

Endereços IPv6 Unicast

Agregatable Global Unicast Address (visão simplificada)

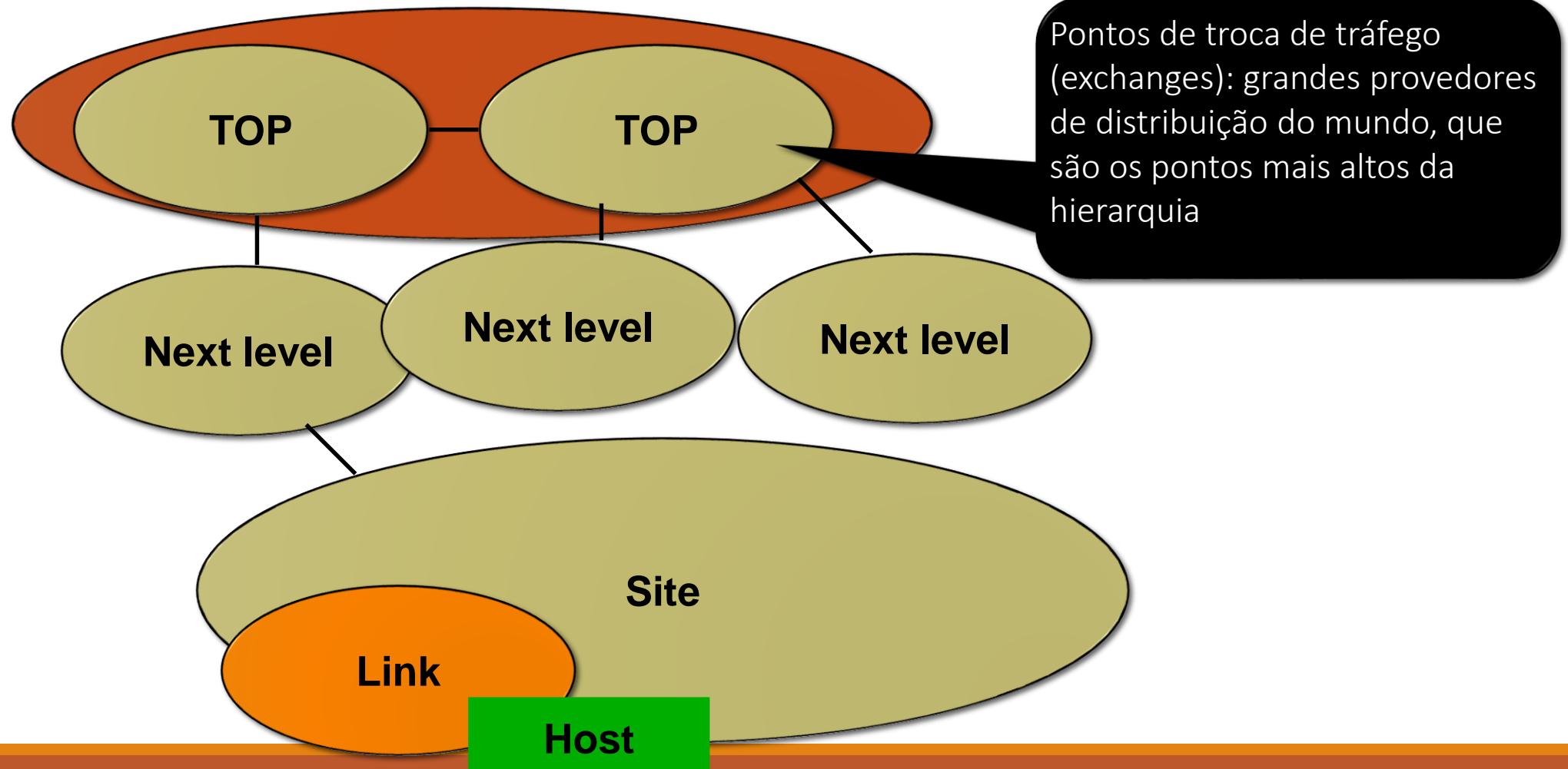
- Equivalente ao endereço global unicast usado em IPv4
 - Estrutura de endereços globais permite uma agregação de prefixos de roteamento que limitam o número de entradas nas tabelas de rotas



- **FP – Format Prefix**, indica que se trata de um endereço do tipo Global Unicast.
- **Global Routing Prefix**, destina a identificação dos ISP's – Internet Service Provider
- **Subnet ID**, o campo Site ID da estrutura de hierarquização do endereço IPv6
- **Interface ID**, identifica a interface do host destino.

Endereços IP Unicast

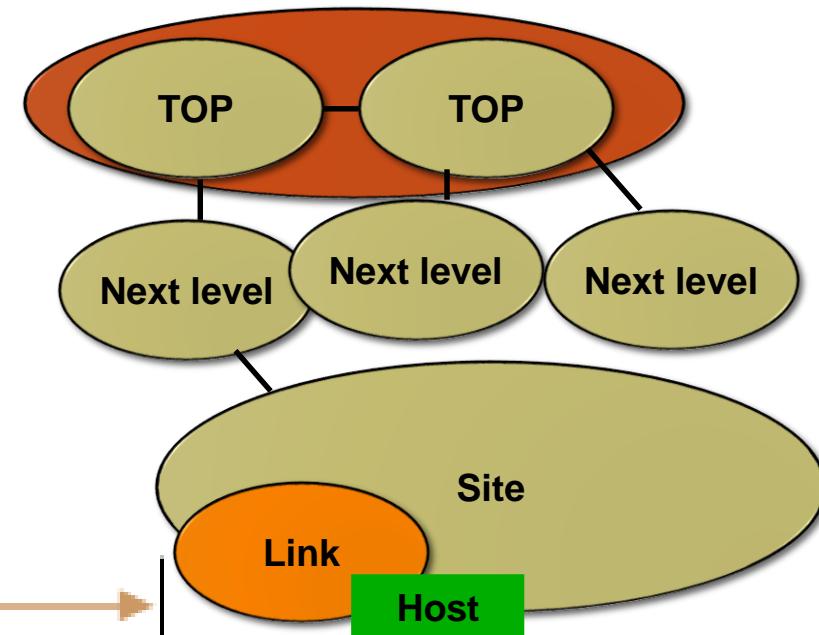
Estrutura hierárquica de roteamento:



Endereços IPv6 Unicast

Endereços unicast globais agregáveis (Aggregatable Global Unicast Addresses)

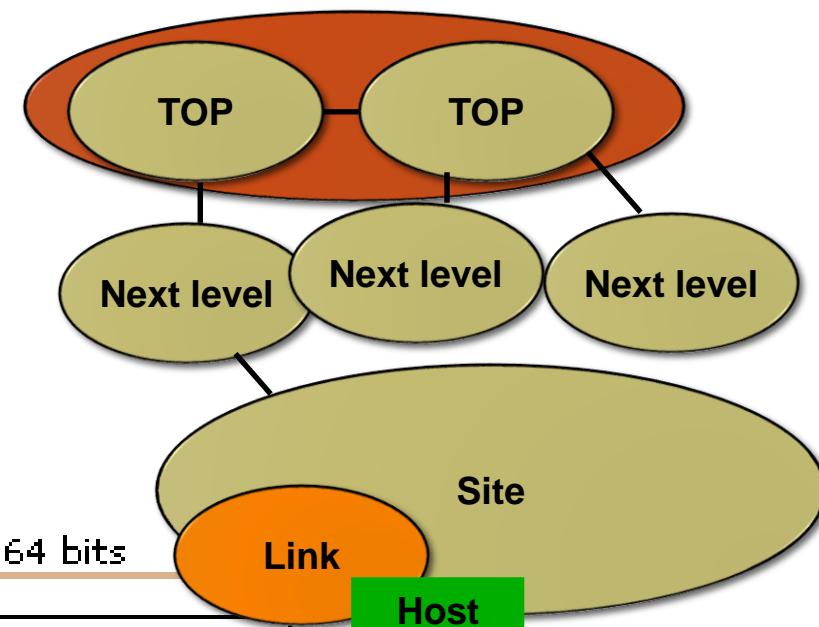
- Estrutura hierárquica existem 4 níveis:
 - TLA ID - Identificador Top-Level Aggregation;
 - NLA ID - Identificador Next-Level Aggregation;
 - SLA ID - Identificador Site-Level Aggregation;
 - Interface ID - Identificador de Interface



Endereços IPv6 Unicast

Top-Level Aggregation ID

- Os identificadores TLA são o topo da hierarquia de roteamento.
- Suporta 8.192 ou (2^{13}) identificadores TLA.
 - Esse campo pode ser aumentado através de um espaço previamente reservado
- Administrados pela IANA e atribuídos a registros de Internet locais (NIC.br) que, por sua vez, atribuem IDs de TLA individuais a fornecedores de serviços Internet (ISP, Internet Service Provider) globais de grandes dimensões
- Os roteadores devem ter uma entrada na tabela de roteamento para cada TLA ID ativo



Endereços IPv6 Unicast

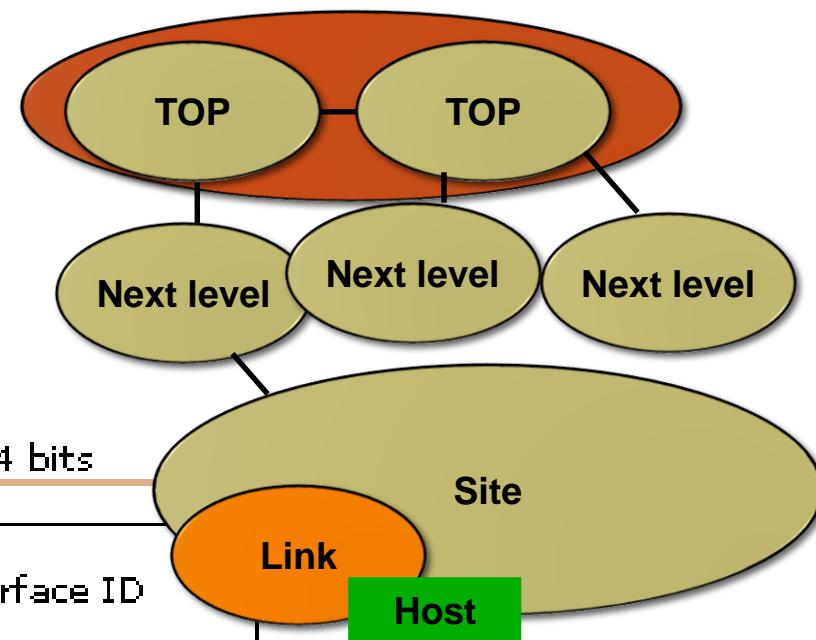
Next-Level Aggregation ID



Endereços IPv6 Unicast

Site-Level Aggregation ID

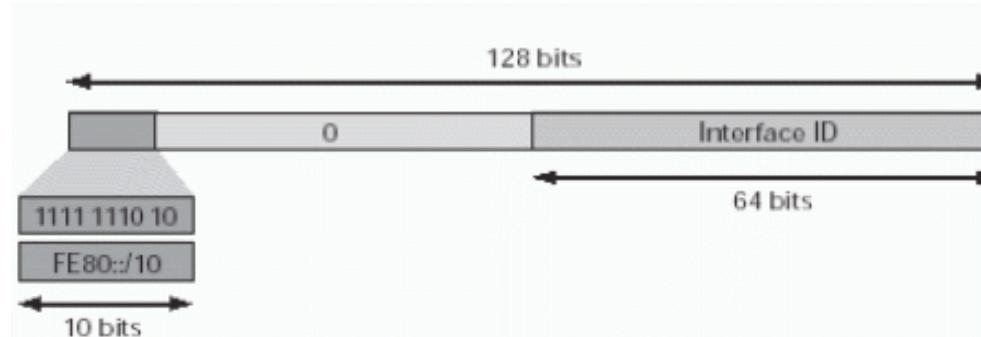
- Utilizado por uma organização individual para identificar sub-redes no respectivo local
- Organização pode utilizar estes 16 bits no respectivo local para criar 65.536 sub-redes ou vários níveis de hierarquia de endereçamento
- Equivalente a uma rede Classe A no IPv4



Endereços IPv6 Unicast

Endereços de enlace local

- Automaticamente configurado em qualquer host IPv6
- Utilizados pelos nós ao comunicar com nós vizinhos no mesmo enlace
 - Numa rede IPv6 de um único enlace sem roteador, os endereços locais de ligação são utilizados para comunicar entre nós do enlace
 - Equivalentes aos endereços IPv4 de endereçamento IP privado automático
 - Um endereço local de enlace é necessário para os processos de identificação de vizinhança
- Um roteador do IPv6 nunca reencaminha o tráfego local de ligação para além da ligação.



Pontos Importantes

Protocolo IPv6

- Conhecer características apresentadas

CAP 6. CAMADA DE REDE

AULA 14: ICMPV6, MOBILIDADE E SEGURANÇA

INE5422 REDES DE COMPUTADORES II

PROF. ROBERTO WILLRICH (INE/UFSC)

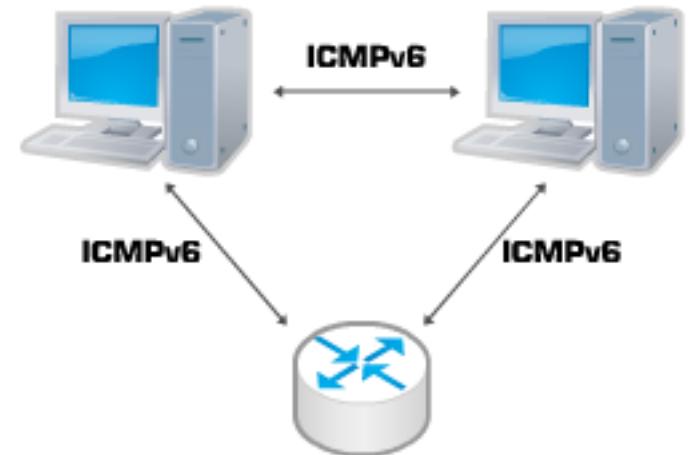
ROBERTO.WILLRICH@UFSC.BR

[HTTPS://MOODLE.UFSC.BR](https://moodle.ufsc.br)

ICMPv6

ICMPv6

- Inclui as mesmas funções básicas do ICMPv4
 - Informar características da rede
 - Diagnósticos
 - Informar erros no processamento e envio dos pacotes
- Dois tipos (classes) de mensagens
 - Mensagens de informação
 - Mensagens de erro



ICMPv6

Apresenta uma quantidade maior de mensagens que a versão ICMP v4

- Além das funções básicas do ICMP são incluídas:
 - Descoberta de vizinhança
 - Incorporadas funções dos protocolos ARP/RARP
 - Gerenciamento de grupo Multicast
 - IGMP (Internet Group Management Protocol)
 - Mobilidade IPv6
 - Descoberta do Path MTU

ICMPv6

Algumas mensagens de erro :

| Mensagens de Erro: | | |
|---------------------------|--------------------------------|---|
| Tipo | Nome | Descrição |
| 1 | <i>Destination Unreachable</i> | Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação. |
| 2 | <i>Packet Too Big</i> | Indica que o tamanho do pacote é maior que a Unidade Máxima de Transito (MTU) de um enlace. |
| 3 | <i>Time Exceeded</i> | Indica que o Limite de Roteamento ou o tempo de remontagem do pacote foi excedido. |
| 4 | <i>Parameter Problem</i> | Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no campo Próximo Cabeçalho não foi reconhecido. |
| 100-101 | | Uso experimental. |
| 102-126 | | Não utilizado. |
| 127 | | Reservado para expansão das mensagens de erro ICMPv6. |

ICMPv6

Algumas mensagens de informação:

| Mensagens de Informação: | | |
|--------------------------|---|--|
| Tipo | Nome | Descrição |
| 128 | <i>Echo Request</i> | Utilizadas pelo comando ping. |
| 129 | <i>Echo Reply</i> | |
| 130 | <i>Multicast Listener Query</i> | |
| 131 | <i>Multicast Listener Report</i> | Utilizadas no gerenciamento de grupos multicast. |
| 132 | <i>Multicast Listener Done</i> | |
| 133 | <i>Router Solicitation</i> | |
| 134 | <i>Router Advertisement</i> | |
| 135 | <i>Neighbor Solicitation</i> | Utilizadas com o protocolo Descoberta de Vizinhança. |
| 136 | <i>Neighbor Advertisement</i> | |
| 137 | <i>Redirect Message</i> | |
| 138 | <i>Router Renumbering</i> | Utilizada no mecanismo de Re-endereçamento (Renumbering) de roteadores. |
| 139 | <i>ICMP Node Information Query</i> | Utilizadas para descobrir informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de redes. |
| 140 | <i>ICMP Node Information Response</i> | |
| 141 | <i>Inverse Neighbor Discovery Solicitation Message</i> | Utilizadas em uma extensão do protocolo de Descoberta de Vizinhança. |
| 142 | <i>Inverse Neighbor Discovery Advertisement Message</i> | |

ICMPv6

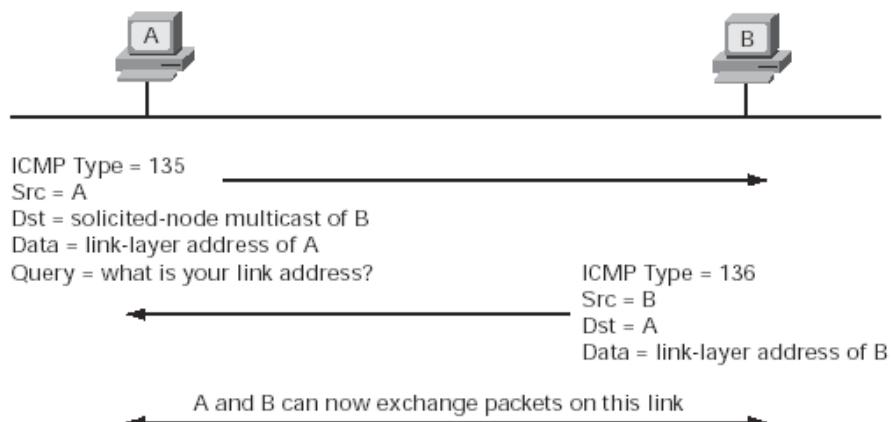
Algumas mensagens de informação:

| | | |
|---------|---|--|
| 144 | <i>Home Agent Address Discovery Request Message</i> | Utilizadas no mecanismo de Mobilidade IPv6. |
| 145 | <i>Home Agent Address Discovery Reply Message</i> | |
| 146 | <i>Mobile Prefix Solicitation</i> | |
| 147 | <i>Mobile Prefix Advertisement</i> | |
| 148 | <i>Certification Path Solicitation Message</i> | Utilizadas pelo protocolo SEND. |
| 149 | <i>Certification Path Advertisement Message</i> | |
| 150 | | Utilizada experimentalmente com protocolos de mobilidade como o Seamoby. |
| 151 | <i>Multicast Router Advertisement</i> | Utilizadas pelo mecanismo Multicast Router Discovery. |
| 152 | <i>Multicast Router Solicitation</i> | |
| 153 | <i>Multicast Router Termination</i> | |
| 154 | <i>FMIPv6 Messages</i> | Utilizada pelo protocolo de mobilidade Fast Handovers |
| 200-201 | | Uso Experimental |
| 255 | | Reservado para expansão das mensagens de erro ICMPv6 |

ICMPv6

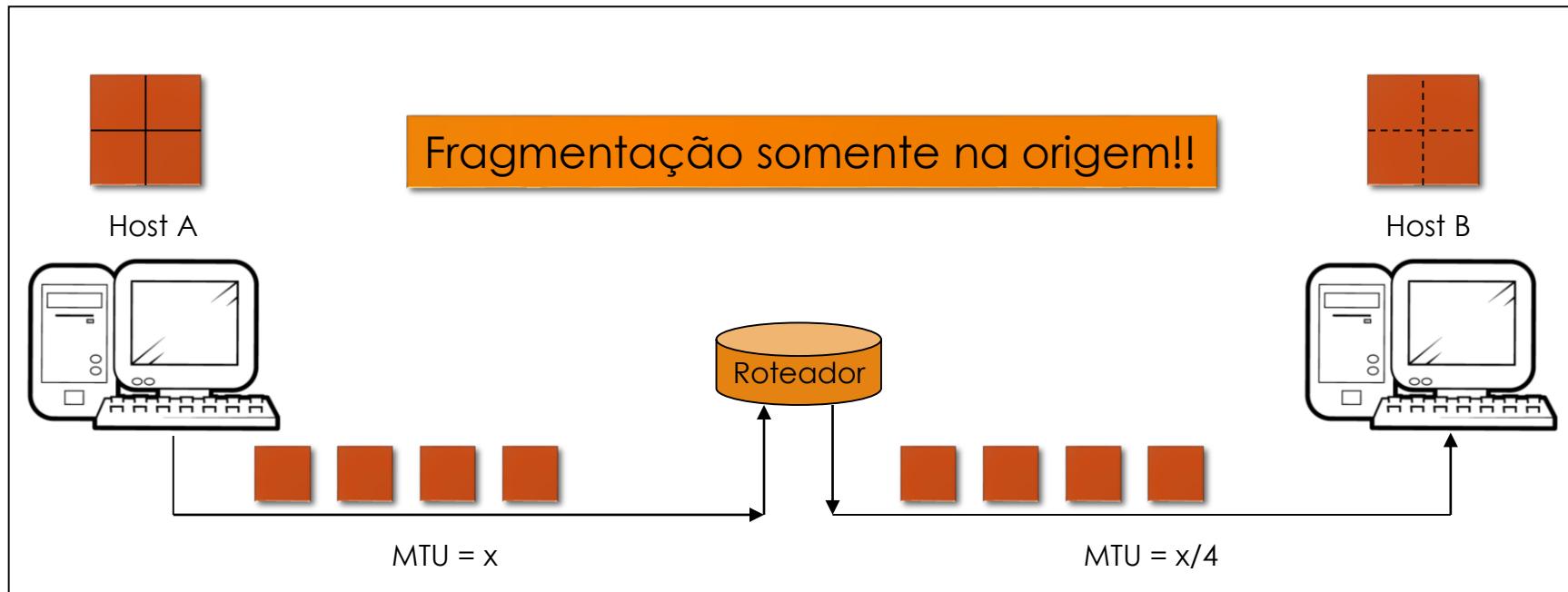
Descoberta de vizinhança

- Descoberta de endereços da camada de enlace
 - Determina o endereço MAC dos vizinhos do mesmo enlace.
 - Neighbor Solicitation (tipo 135): mensagem multicast enviada pelos nós para determinar endereço MAC e acessibilidade de um vizinho. Também pode detectar endereços duplicados.
 - Neighbor Advertisement (tipo 136): é uma mensagem unicast enviada como resposta a uma Neighbor Solicitation. Pode ser enviada periodicamente em multicast para todos os demais.
 - Substitui o protocolo ARP do IPv4, utilizando um endereço multicast como destino



ICMPv6

IPv6 diminui-se o overhead dos roteadores, pois a fragmentação é realizada na origem



ICMPv6

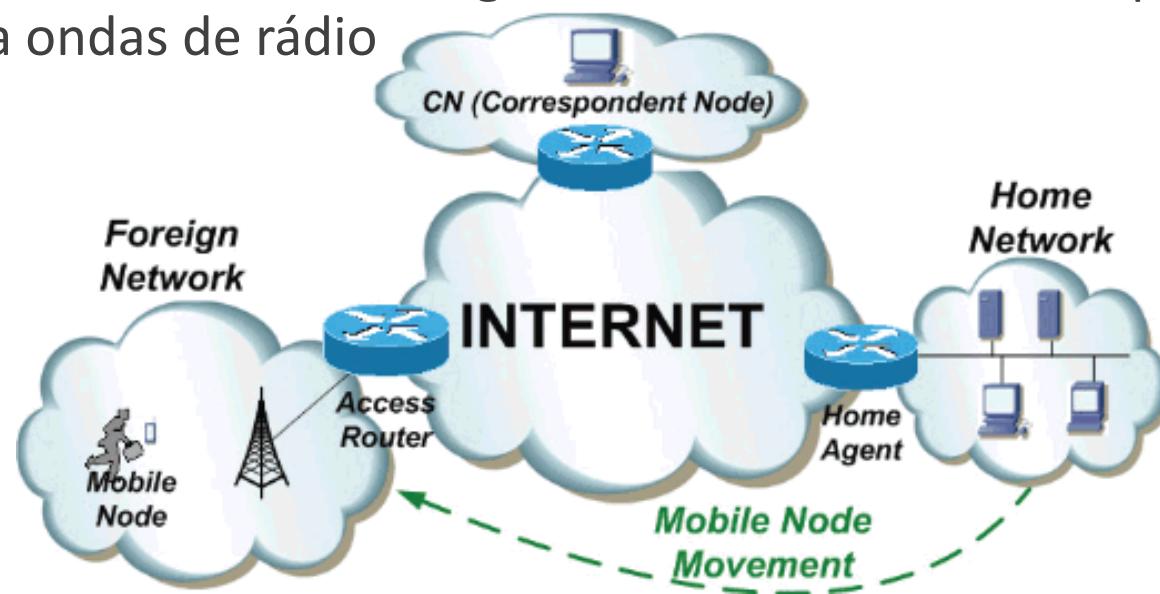
Path MTU Discovery

- Assume que o MTU é o mesmo MTU do enlace inicial
- Se, no caminho, o tamanho de qualquer pacote for maior que o MTU informado pelo roteador do próximo enlace, o roteador descarta o pacote, e retorna um *ICMPv6 packet too big*
- Este mecanismo continua até que o tamanho do pacote seja igual ou menor ao menor MTU do caminho, realizando quantas reduções forem necessárias

Mobilidade IPv6

Necessidades, Metas e Aplicações

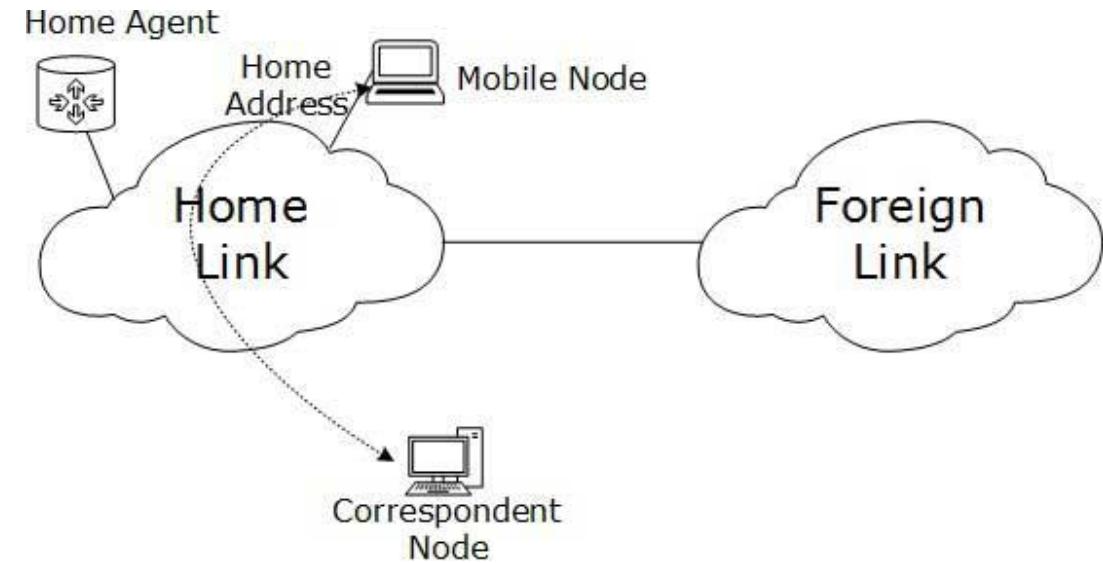
- Suporte a mobilidade no IPv6 provê mecanismos para que um nó possa mudar de uma rede para outra de forma transparente ao usuário.
- Estas redes não precisam necessariamente ser homogêneas: pode ocorrer do host mudar de rede e de forma de acesso.
- Nó ligado num momento a um segmento Ethernet, e em um próximo instante estar conectado via ondas de rádio



Mobilidade IPv6

Protocolo deve manter a comunicação com outros nós após a mudança de sub-rede do nó móvel

- O mobile node deve sempre ser acessível através de seu endereço de origem (home address)
 - Um endereço permanente
 - os pacotes enviados para este endereço devem ser repassados para a posição atual do mobile node.
- Home Agent: roteador que age como um registrador de dispositivos móveis e mantém informações sobre todos os nós móveis (seus Home Address e seu IP atual)

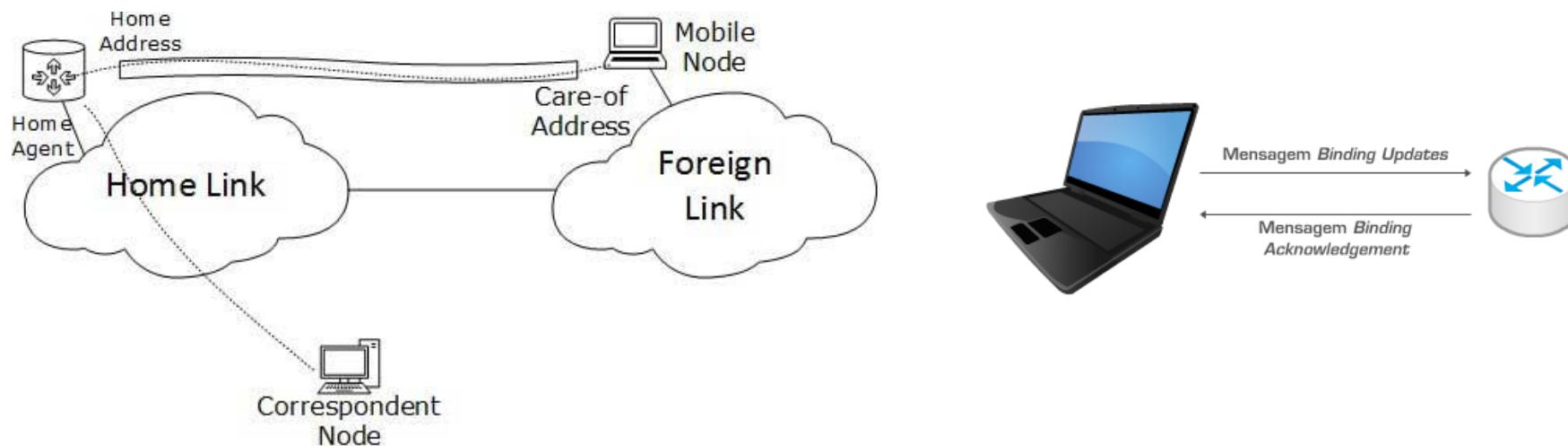


Mobilidade IPv6

A mudança de sub-rede do host deve ser transparente para a camadas de transporte e superiores.

Quando nó móvel se desloca para fora de sua rede de origem

- Obtêm um care-of address
- Para que os pacotes cheguem neste novo endereço é necessária uma associação entre o home address e o care-of address
- Associação chamada de binding
- Feita por um *Home Agent* (roteador na rede de origem)



Segurança IPv6

Segurança IPv4

- IPv4 foi projetado para redes acadêmicas, que após utilizada como estrutura de comunicação comercial produziu problemas de segurança
- IPSec
 - Protocolo que implementa criptografia e autenticação no IPv4, garantindo:
 - Que a mensagem recebida não tenha sido adulterada;
 - A identidade do remetente;
 - A confidencialidade da mensagem, criptografando seu conteúdo
 - Mecanismo de autenticação não pode ser utilizado em conexões que estejam atrás de NAT

Segurança IPv6

Segurança IPv6

- Implantação do IPSec é mais simples e tem as mesmas funções do IPv4:
 - Não há necessidade de se usar NAT permitindo que o IPSec funcione sem restrições;
 - Mecanismos de autenticação e encapsulamento do IPSec fazem parte do protocolo
 - Seu suporte é obrigatório em todos os nós (que não ocorre no IPv4)

Pontos Importantes

Alguns aspectos do IPv6

- Conhecer aspectos relacionados à fragmentação, mobilidade e segurança