

PTC 2550 - Aula 05

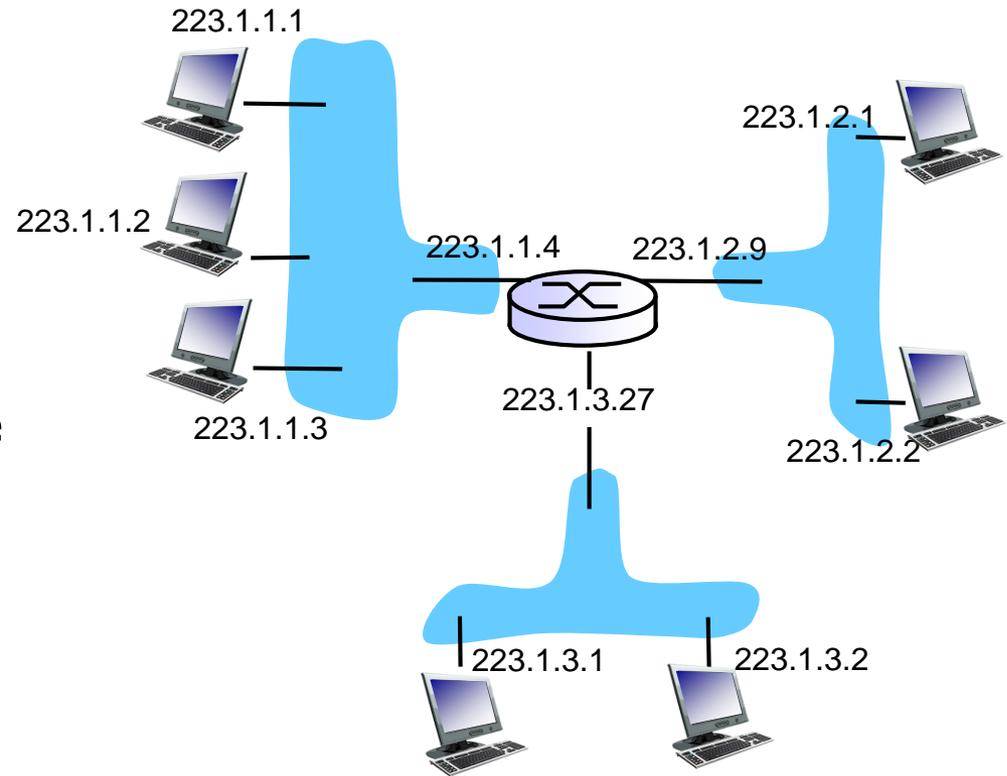
I.4 A camada de rede (2/2)

(Kurose, p. 224 - 306)

24/03/2017

Endereçamento IP : introdução

- ❖ **endereço IP :**
identificador de 32 bits para *interfaces* de *hosts* e roteadores
- ❖ **interface:** conexão entre *host* ou roteador e enlace físico
 - roteador tipicamente têm múltiplas interfaces
 - *host* tipicamente tem 1 ou duas interfaces (e.g., Ethernet cabeada, 802.11 sem fio)
- ❖ **endereços IP associados com cada interface – aprox. 4 bilhões de interfaces**



$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_1 \underbrace{00000001}_1 \underbrace{00000001}_1$$

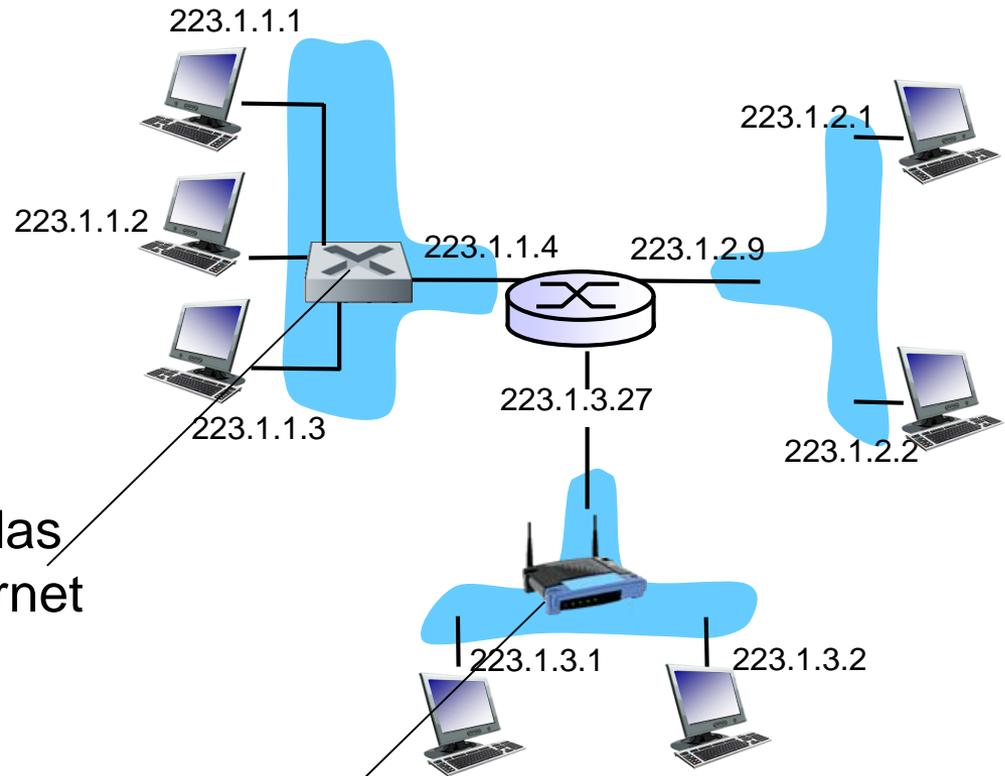
Endereçamento IP : introdução

Q: como as interfaces são de fato conectadas?

R: Assunto da camada de rede – *Próximas aulas!*

R: interfaces Ethernet cabeadas conectadas a switches Ethernet

Por hora: não precisamos nos preocupar em como as interfaces se conectam (sem roteador interveniente)



R: interfaces WiFi sem fio conectadas a estação base WiFi

Sub-redes

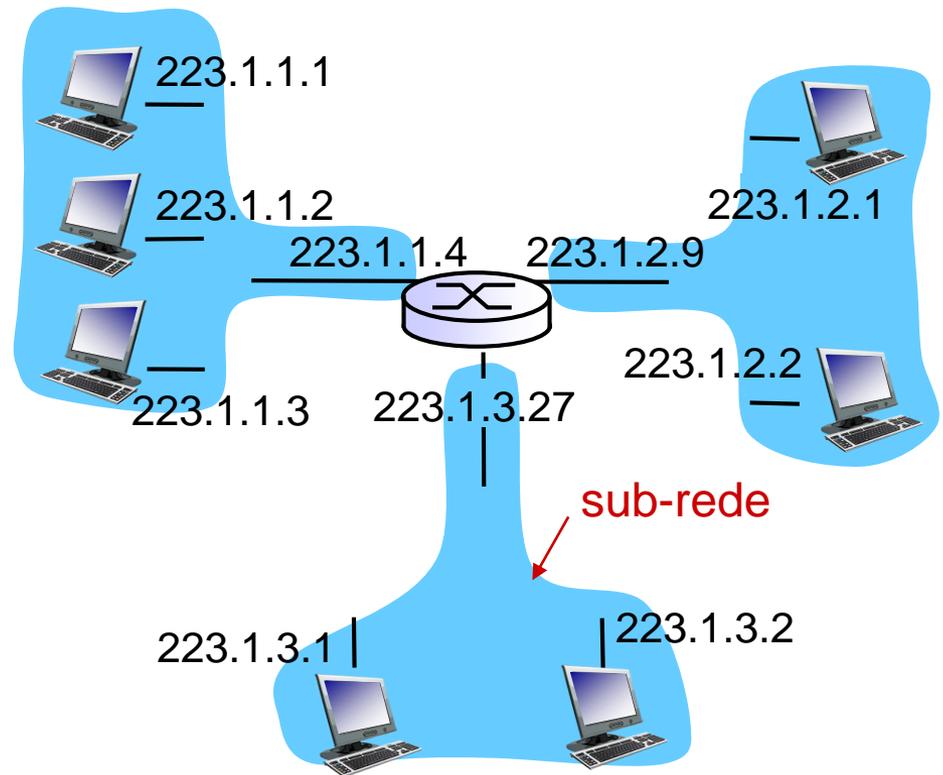
Com os prefixos **sub** e **sob**, usa-se o hífen diante de palavra iniciada por r. Exemplos: sub-região sub-reitor sub-regional sob-roda

❖ endereço IP :

- parte sub-rede - bits de ordem mais alta
- parte *host* - bits de ordem mais baixa

❖ o que é uma sub-rede ?

- interfaces de dispositivos com mesma parte sub-rede do endereço IP
- podem alcançar-se fisicamente *sem passar por roteador*

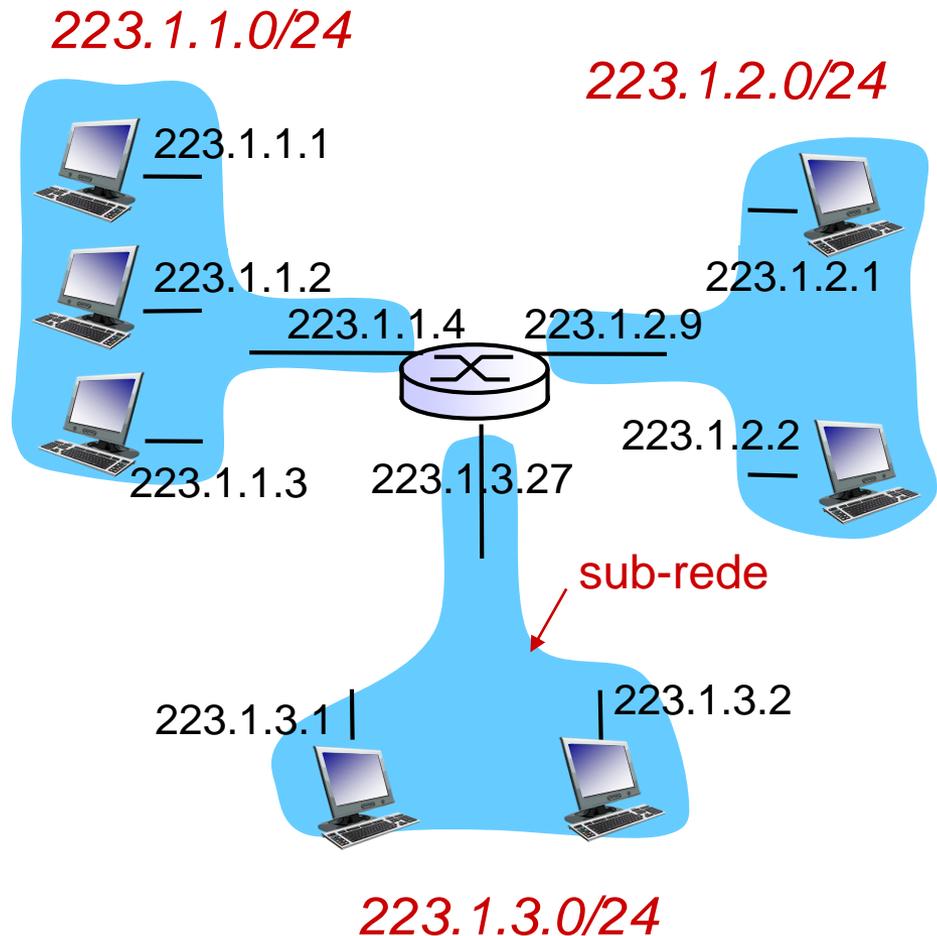


rede consistindo de 3 sub-redes

Sub-redes

receita

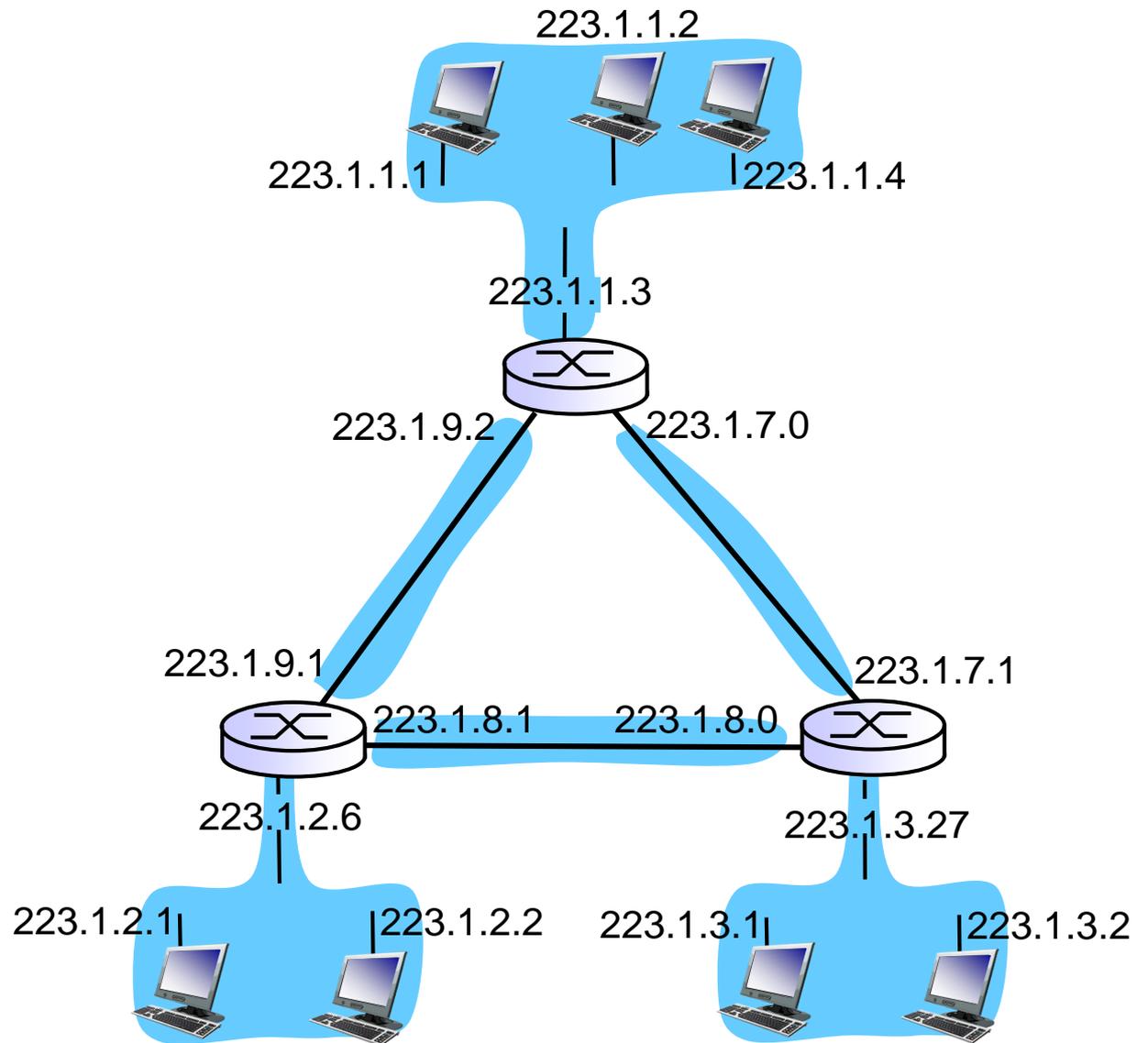
- ❖ para determinar as sub-redes, separe cada interface do seu *host* ou roteador, criando ilhas de redes isoladas
- ❖ cada rede isolada é chamada de *sub-rede*



mascara de sub-rede : /24

Sub-redes

Quantas?



Endereçamento IP : CIDR [[RFC1338 \(1992\)](#)...[RFC4632 \(2006\)](#)]

CIDR: *Classless InterDomain Routing* (sáider)

- porção sub-rede do endereço tem comprimento arbitrário (prefixo)
- formato do endereço: **a.b.c.d/x**, sendo x # bits na porção sub-rede do endereço



- *Máscara: 255.255.254.0*
- **Endereço de difusão reservado: 255.255.255.255**

Endereços IP : como conseguir um?

Q: Como um *host* obtém um endereço IP?

- ❖ colocado pelo administrador do sistema
 - **Windows:** painel de controle->central de redes e compartilhamento->alterar as configurações do adaptador->tcp/ip-> propriedades
 - **OSX:** preferências do sistema -> Rede -> Configurar IPv4
- ❖ **DHCP: *D*ynamic *H*ost *C*onfiguration *P*rotocol:** obtém endereço dinamicamente de um servidor
 - protocolo cliente-servidor da camada de aplicação
 - usa UDP e IP
 - “*plug-and-play*”

DHCP: Dynamic Host Configuration Protocol [RFC 1541(1993) - 2131]

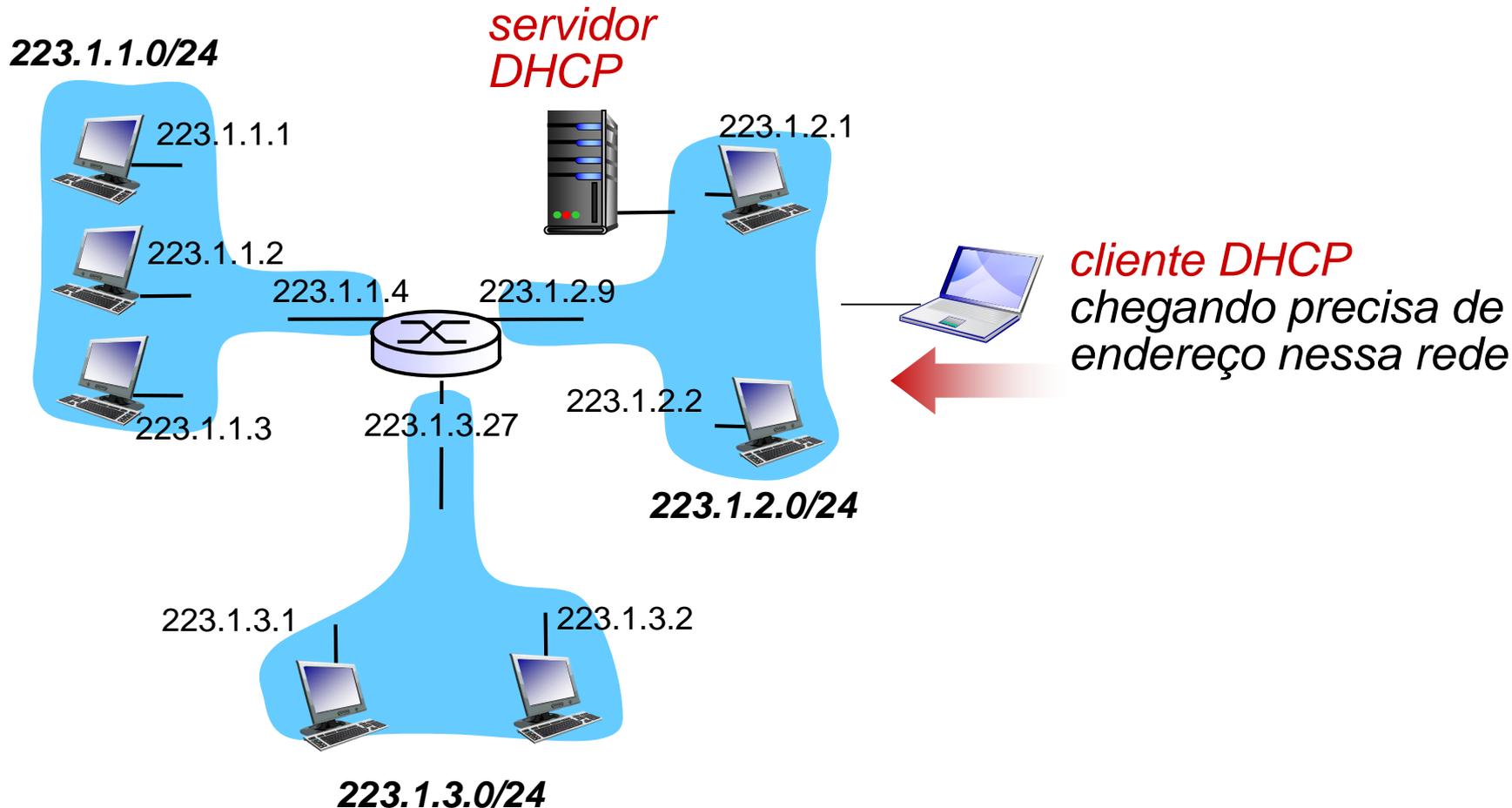
objetivo: permitir a *host* obter dinamicamente seu endereço IP de um servidor de rede quando ele se junta à rede

- permite reuso de endereços (apenas mantém endereço enquanto conectado / ligado) – endereço IP temporário
- também permite que *host* receba mesmo IP sempre que se conectar
- pode renovar sua concessão do endereço em uso

Visão geral do DHCP :

- *host* *difunde* (ainda não sabe IP do servidor): mensagem “DHCP discover”
- servidor DHCP responde com mensagem “DHCP offer”
- *host* requer endereço IP : mensagem “DHCP request”
- servidor DHCP envia endereço: mensagem “DHCP ack”

Cenário cliente-servidor DHCP



Cenário DHCP cliente-servidor

servidor DHCP : 223.1.2.5

DHCP discover

```
src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654
```

cliente chegando



DHCP offer

```
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs
```

DHCP request

```
src: 0.0.0.0, 68
dest.: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs
```

DHCP ACK

```
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs
```

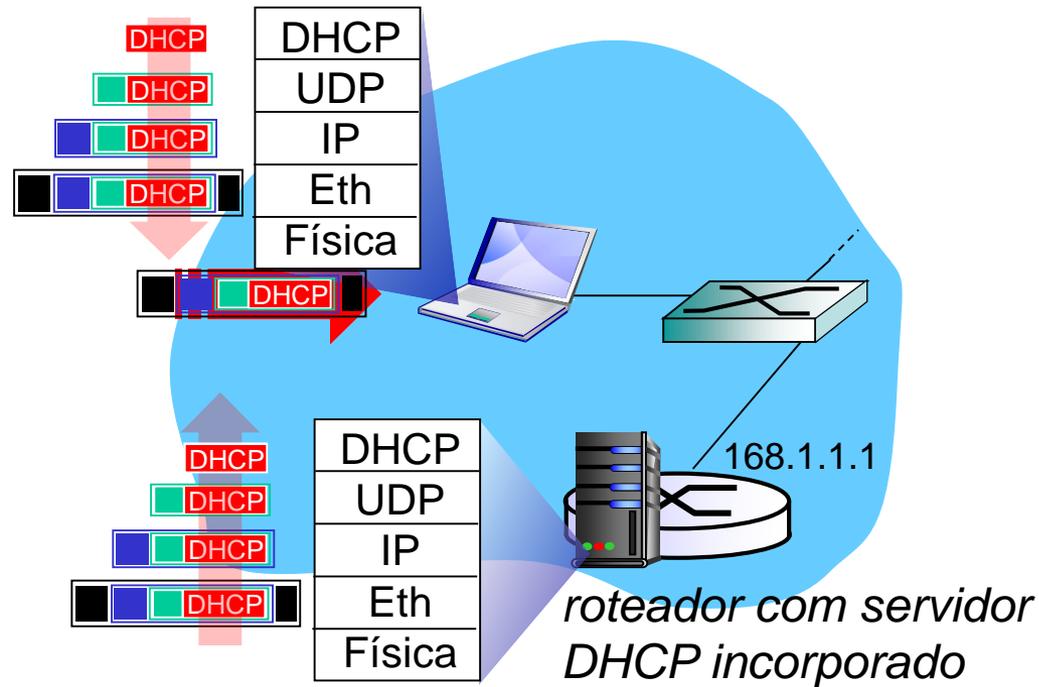
Obs: *yiaddr* =
your internet address

DHCP: mais do que endereços IP

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

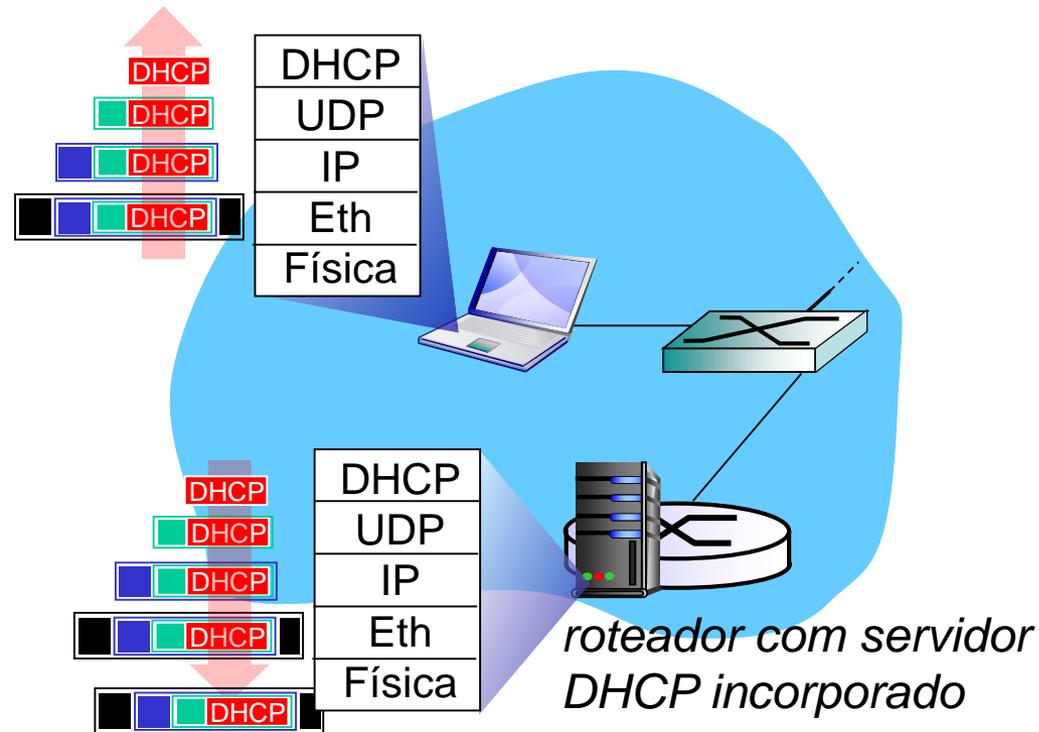
- endereço do roteador de primeiro salto para o cliente
- nome e endereço IP do servidor DNS
- máscara de rede (indicando a parte de sub-rede e a parte *host* do endereço)

DHCP: exemplo



- ❖ *laptop* conectando-se precisa do seu endereço IP, endereço do roteador de primeiro salto, endereço do servidor DNS: usa DHCP
- ❖ pedido DHCP encapsulado em UDP, encapsulado em IP, encapsulado em Ethernet 802.1
- ❖ quadro Ethernet difundido (dest: 255.255.255.255) na LAN, recebido no roteador rodando servidor DHCP
- ❖ Ethernet desmultiplexado para IP desmultiplexado para UDP desmultiplexado para DHCP

DHCP: exemplo



- ❖ servidor DHCP formula DHCP ACK contendo endereço IP, endereço IP do roteador do primeiro salto, nome e endereço IP do servidor DNS
- ❖ encapsulamento do servidor DHCP, quadro repassado ao cliente, desmultiplexado para cima no cliente DHCP
- ❖ cliente sabe agora seu endereço IP, nome e endereço IP do servidor DNS, endereço IP do roteador do primeiro salto

DHCP: saída do Wireshark (LAN doméstica)

Message type: **Boot Request (1)**

Hardware type: Ethernet
Hardware address length: 6
Hops: 0

Transaction ID: 0x6b3a11b7

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 0.0.0.0 (0.0.0.0)

Next server IP address: 0.0.0.0 (0.0.0.0)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Server host name not given

Boot file name not given

Magic cookie: (OK)

Option: (t=53,l=1) **DHCP Message Type = DHCP Request**

Option: (61) Client identifier

Length: 7; Value: 010016D323688A;

Hardware type: Ethernet

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Option: (t=50,l=4) Requested IP Address = 192.168.1.101

Option: (t=12,l=5) Host Name = "nomad"

Option: (55) Parameter Request List

Length: 11; Value: 010F03062C2E2F1F21F92B

1 = Subnet Mask; 15 = Domain Name

3 = Router; 6 = Domain Name Server

44 = NetBIOS over TCP/IP Name Server

.....

pedido

Message type: **Boot Reply (2)**

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x6b3a11b7

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.1.101 (192.168.1.101)

Your (client) IP address: 0.0.0.0 (0.0.0.0)

Next server IP address: 192.168.1.1 (192.168.1.1)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)

Server host name not given

Boot file name not given

Magic cookie: (OK)

Option: (t=53,l=1) DHCP Message Type = DHCP ACK

Option: (t=54,l=4) Server Identifier = 192.168.1.1

Option: (t=1,l=4) Subnet Mask = 255.255.255.0

Option: (t=3,l=4) Router = 192.168.1.1

Option: (6) Domain Name Server

Length: 12; Value: 445747E2445749F244574092;

IP Address: 68.87.71.226;

IP Address: 68.87.73.242;

IP Address: 68.87.64.146

Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

resposta

*Pergunta: O que acontece
se usuário sair
de sub-rede e entrar em
outra durante sessão TCP?*

Endereços IP : como obter um?

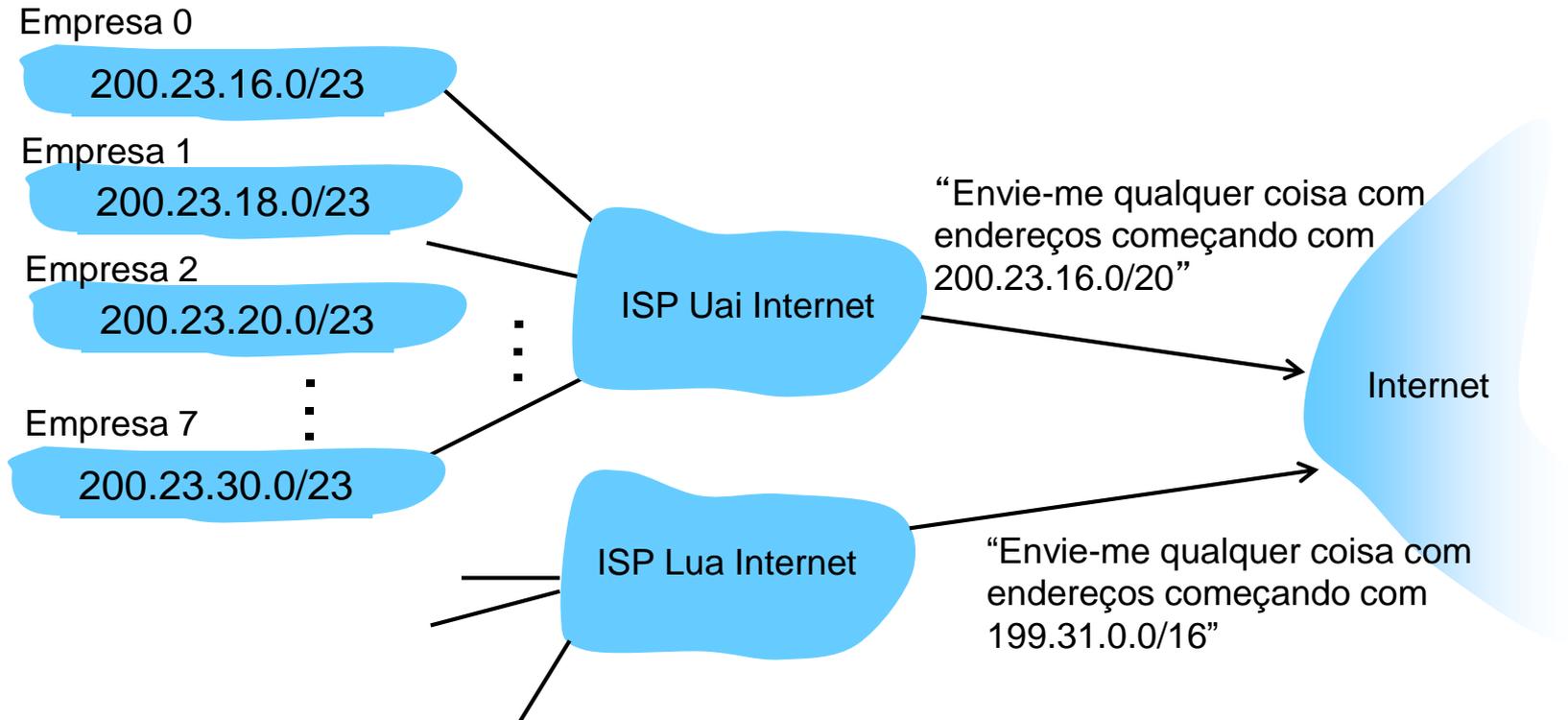
Q: Como uma rede obtém a parte sub-rede do endereço IP?

R: obtém porção alocada do espaço de endereços do seu ISP

Bloco do ISP	<u>11001000 00010111 00010000</u> 00000000	200.23.16.0/20
Empresa 0	<u>11001000 00010111 00010000</u> 00000000	200.23.16.0/23
Empresa 1	<u>11001000 00010111 00010010</u> 00000000	200.23.18.0/23
Empresa 2	<u>11001000 00010111 00010100</u> 00000000	200.23.20.0/23
...
Empresa 7	<u>11001000 00010111 00011110</u> 00000000	200.23.30.0/23

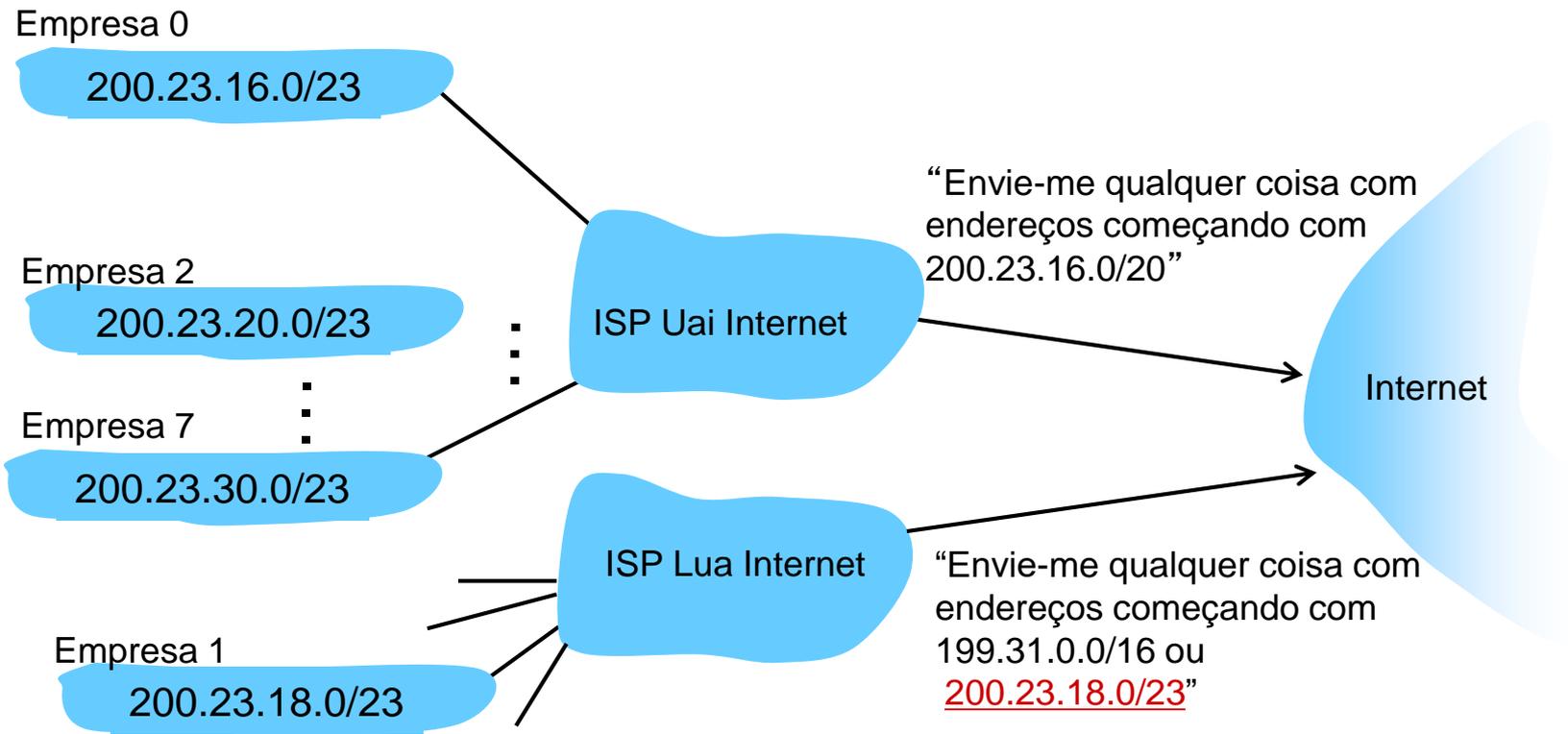
Endereçamento hierárquico : agregação de rotas

endereçamento hierárquico permite anúncio eficiente da informação de roteamento:



Endereçamento hierárquico : rotas mais específicas

Lua Internet tem uma rota mais específica para a Empresa 1



Endereço IP : o último passo...

Q: como um ISP obtém um bloco de endereços?

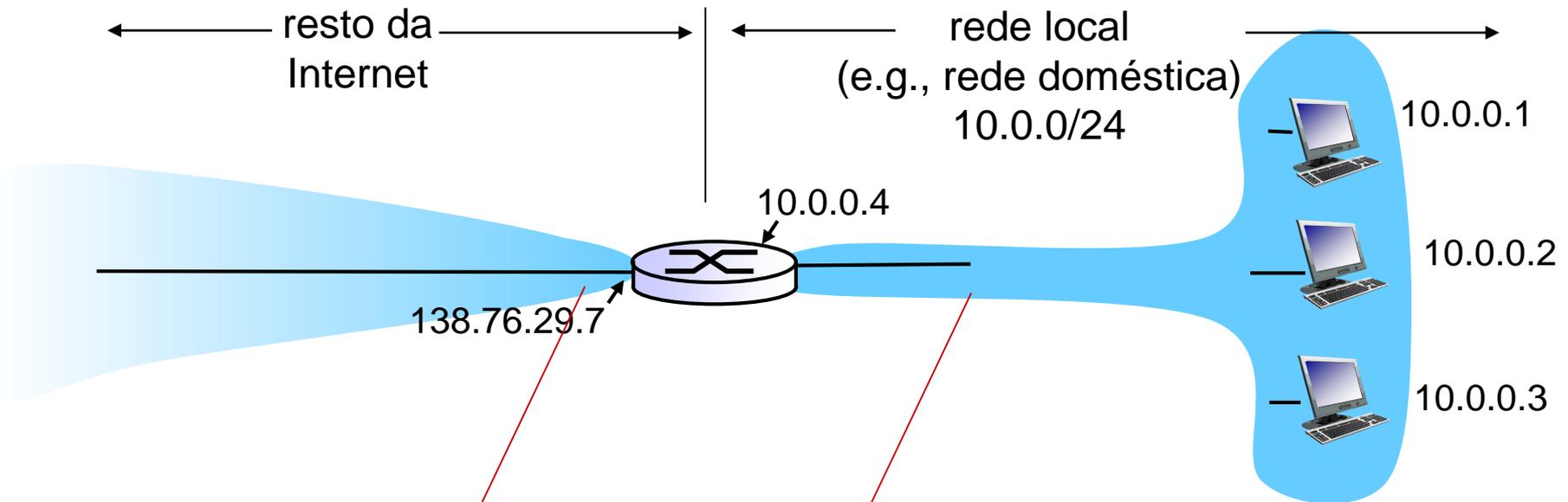
R: ICANN: Internet Corporation for Assigned Names and Numbers <http://www.icann.org/>

- alocação de endereços
- gerenciamento dos DNS raízes
- atribuições de nomes de domínios, resolução de disputas

R: América Latina: <http://www.lacnic.net/>

R: No Brasil: <http://registro.br> (Tecnologia → Provedor de acesso)

NAT: Network Address Translation



todos os datagramas *saem* da rede local com *mesmo* único endereço fonte IP NAT: 138.76.29.7, diferentes números de portas fontes

datagramas com fonte ou destino nessa rede tem endereço 10.0.0/24 para fonte ou destino (como usual)

NAT: Network Address Translation

motivação:

- ❖ rede local inteira usa apenas um único IP do ponto de vista do mundo exterior:
 - não é necessário intervalo de endereços do ISP: apenas um endereço IP para todos os dispositivos
 - pode-se mudar endereços dos dispositivos na rede local sem notificar mundo exterior
 - pode-se mudar ISP sem mudar endereços dos dispositivos na rede local
 - dispositivos na rede local não são explicitamente endereçáveis – invisíveis do ponto de vista do mundo exterior (um aumento na segurança)

NAT: Network Address Translation

implementação: roteador NAT precisa:

- *datagramas saindo: trocar* (endereço IP fonte, # porta) de cada datagrama que sai por (endereço NAT IP, novo # porta)
... clientes/servidores remotos vão responder usando (endereço NAT IP, novo # porta) como endereço destino
- *lembrar (em uma tabela de tradução NAT)* cada par de tradução (endereço IP fonte, # porta) para (endereço NAT IP, novo # porta)
- *datagramas chegando : trocar* (endereço NAT IP, novo # porta) nos campos destino de cada datagrama que chega pelo correspondente (endereço IP fonte, # porta) armazenado na tabela NAT
- RFC1918 – endereços para rede privada: 10/8, 172.16/12 e 192.168/16

NAT: Network Address Translation

tabela de tradução NAT	
end. lado WAN	end. lado LAN
138.76.29.7, 5001	10.0.0.1, 3345
.....

1: host 10.0.0.1 envia datagrama para 128.119.40.186, 80

S: 10.0.0.1, 3345
D: 128.119.40.186, 80

S: 138.76.29.7, 5001
D: 128.119.40.186, 80

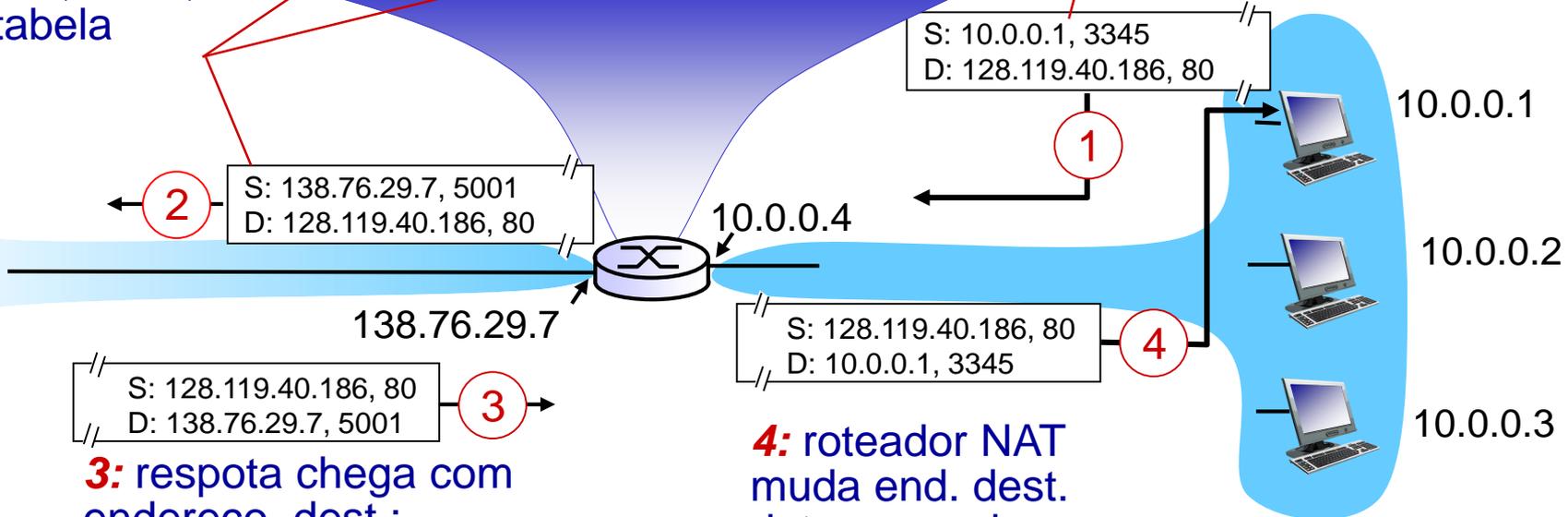
S: 128.119.40.186, 80
D: 138.76.29.7, 5001

S: 128.119.40.186, 80
D: 10.0.0.1, 3345

2: roteador NAT muda end. fonte do datagrama de 10.0.0.1, 3345 para 138.76.29.7, 5001, atualiza tabela

3: resposta chega com endereço dest.: 138.76.29.7, 5001

4: roteador NAT muda end. dest. datagrama de 138.76.29.7, 5001 para 10.0.0.1, 3345

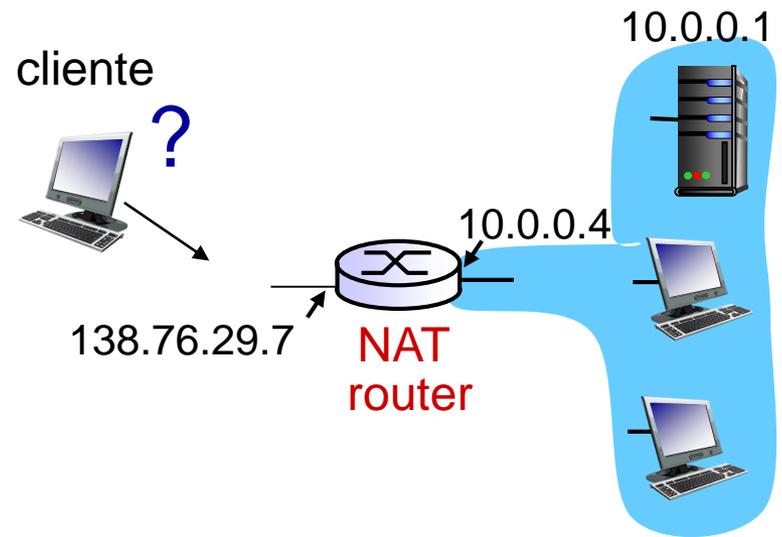


NAT: Network Address Translation

- ❖ campo número de porta tem 16 bits:
 - 60 000 conexões simultâneas com um único endereço do lado WAN!
- ❖ NAT é controverso!
 - roteadores deveriam processar apenas até a camada de rede! Não deveriam acessar # porta!
 - servidores em redes NAT têm problemas!
 - viola argumento fim-a-fim
 - a possibilidade NAT precisa ser levada em conta por projetistas de *apps*, e.g. aplicações P2P
 - falta de endereços deveria ser resolvida usando IPv6

Problema de travessia do NAT

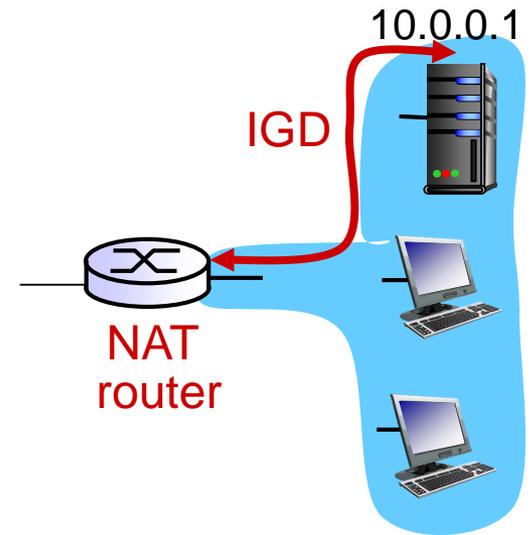
- ❖ cliente quer se conectar a servidor com endereço 10.0.0.1
 - endereço do servidor 10.0.0.1 é local à LAN (cliente não pode usar como endereço destino!)
 - apenas um endereço NAT visível externamente: 138.76.29.7
- ❖ **solução 1**: estaticamente configurar NAT para repassar requisição de conexão que chega em dada porta ao servidor
 - e.g., (138.76.29.7, porta 2500) sempre repassada para 10.0.0.1 porta 25000



Problema de travessia do NAT

- ❖ **solução 2:** Protocolos *Universal Plug and Play (UPnP)* e *Internet Gateway Device (IGD)*. Permite *host atrás do NAT*:
 - ❖ aprender endereço IP público (138.76.29.7)
 - ❖ adicionar/remover mapeamento de portas (com tempo de locação)

i.e., automatiza configuração de mapa de portas NAT estáticas



Problema de travessia do NAT

- ❖ **solução 3:** retransmissão (usado no Skype)
 - cliente atrás de NAT estabelece conexão com retransmissor
 - cliente externo se conecta a retransmissor
 - retransmissor serve de ponte para pacotes entre conexões



IPv6: motivação

- ❖ *motivação inicial*: espaço de endereços de 32 bits em breve estará completamente alocada (percebeu-se no começo da década de 90!)
- ❖ IPv6 – [RFC 1883](#) (dez/1995)... [RFC 7112](#) (jan/2014)
- ❖ Feb. 2011 – IANA alocou último conjunto de endereços IPv4 a registrador regional
- ❖ Feb. 2017 – [LACNIC anuncia esgotamento de endereços para América do Sul e Caribe](#)
- ❖ *motivações adicionais*:
 - formato de cabeçalho ajuda a aumentar velocidade de processamento/repasse
 - cabeçalho muda para facilitar QoS

formato datagrama IPv6 :

- cabeçalho de comprimento fixo 40 bytes
- não é permitida fragmentação

Endereços IPv6

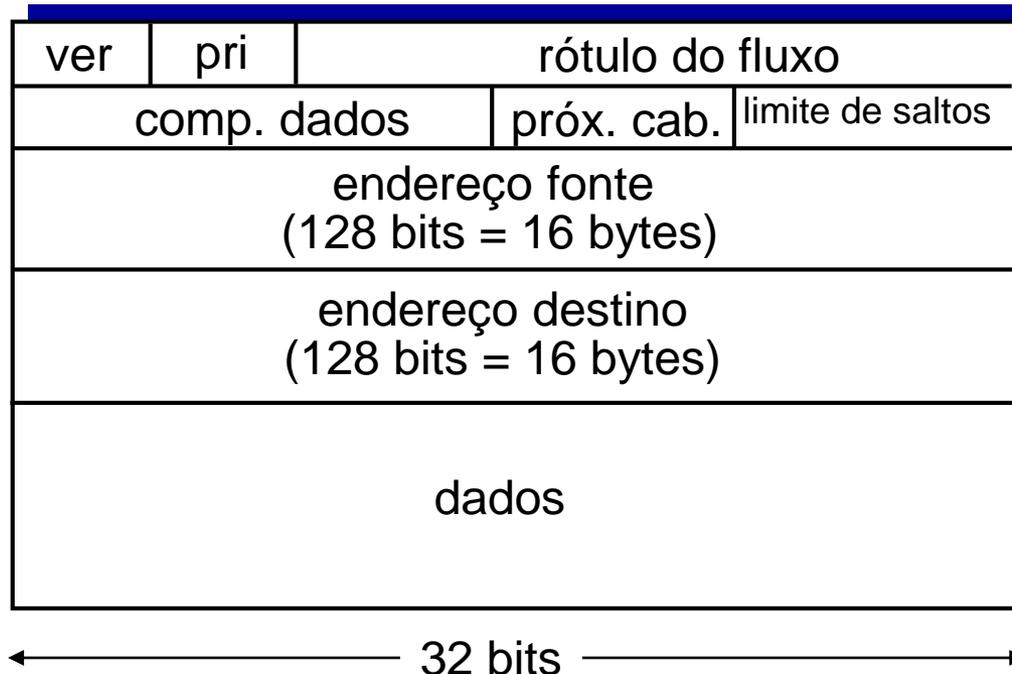
- ❖ Endereços com 128 bits ou 16 bytes
 - ❖ Permite $3,4 \times 10^{38}$ endereços!
 - ❖ Existem da ordem de [10²² estrelas no universo](#)
 - ❖ Existem da ordem de [10²² grãos de areia na Terra](#)
 - ❖ Os endereços IPv6 são escritos como oito grupos de 4 dígitos hexadecimais.
 - ❖ Por exemplo,
 - `2001:0db8:85a3:08d3:1319:8a2e:0370:7344`
 - ❖ Se um grupo de vários dígitos seguidos for 0000, pode ser omitido.
 - ❖ Por exemplo,
 - `2001:0db8:85a3:0000:0000:0000:0000:7344`
- é o mesmo endereço IPv6 que:
- `2001:0db8:85a3::7344`

Formato do datagrama IPv6

prioridade: identifica prioridade entre fluxo de datagramas (8 bits)

rótulo do fluxo: identifica datagramas no mesmo “fluxo.” (20 bits)
(conceito de “fluxo” ainda não bem definida).

próximo cabeçalho: identifica protocolo da camada superior para dados

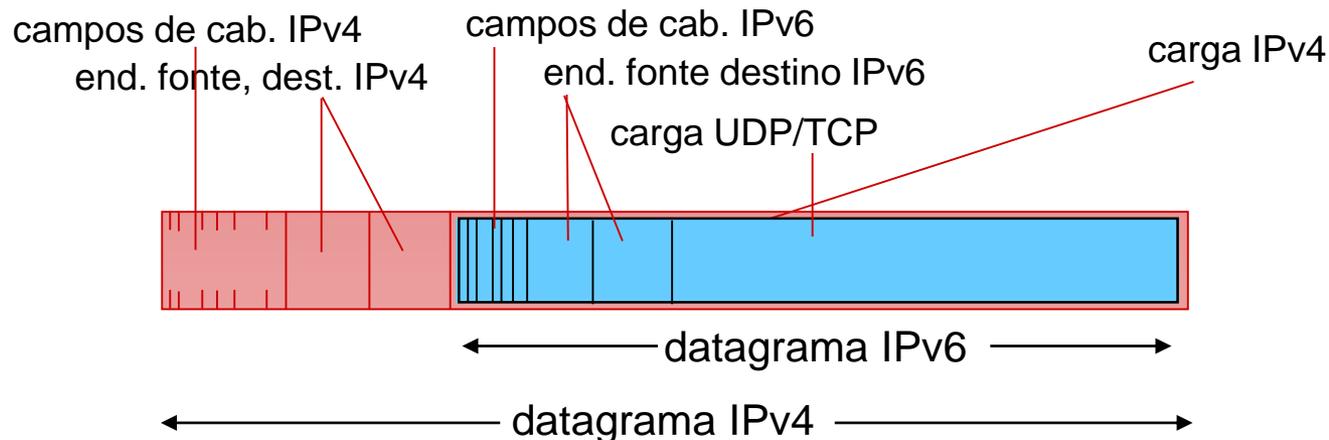


Outras mudanças em relação ao IPv4

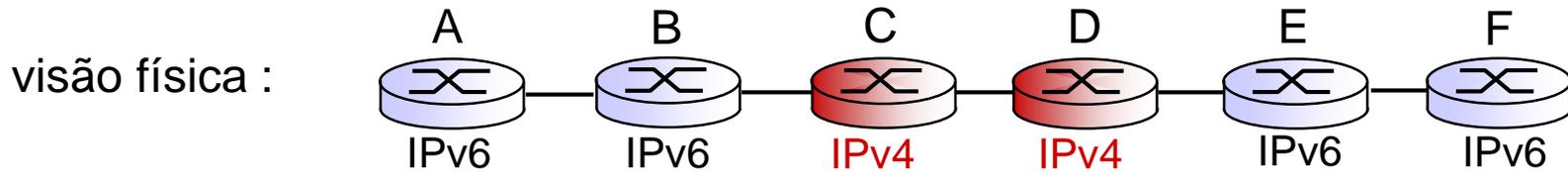
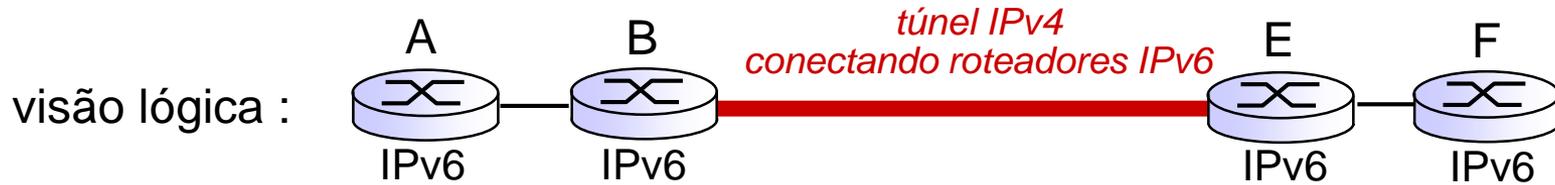
- ❖ *checksum*: removido inteiramente para reduzir o tempo de processamento em cada salto
- ❖ *opções*: permitidas, mas fora do cabeçalho, indicado pelo campo “Próximo Cabeçalho”
- ❖ *ICMPv6*: nova versão do ICMP [[RFC 2463](#) (1998) ... [RFC 4884](#) (2007)]
 - tipos de mensagens adicionais, e.g. “Pacote Muito Grande”
 - incorpora funções de gerenciamento de grupos *multicast* ([IGMP](#))

Transição do IPv4 para IPv6

- ❖ nem todos os roteadores podem ser atualizados simultaneamente
 - sem “dia D”
 - Como a rede opera com roteadores IPv4 e IPv6 misturados?
- ❖ **tunelamento**: datagrama IPv6 carregado como dados em datagrama IPv4 entre roteadores IPv4



Tunelamento

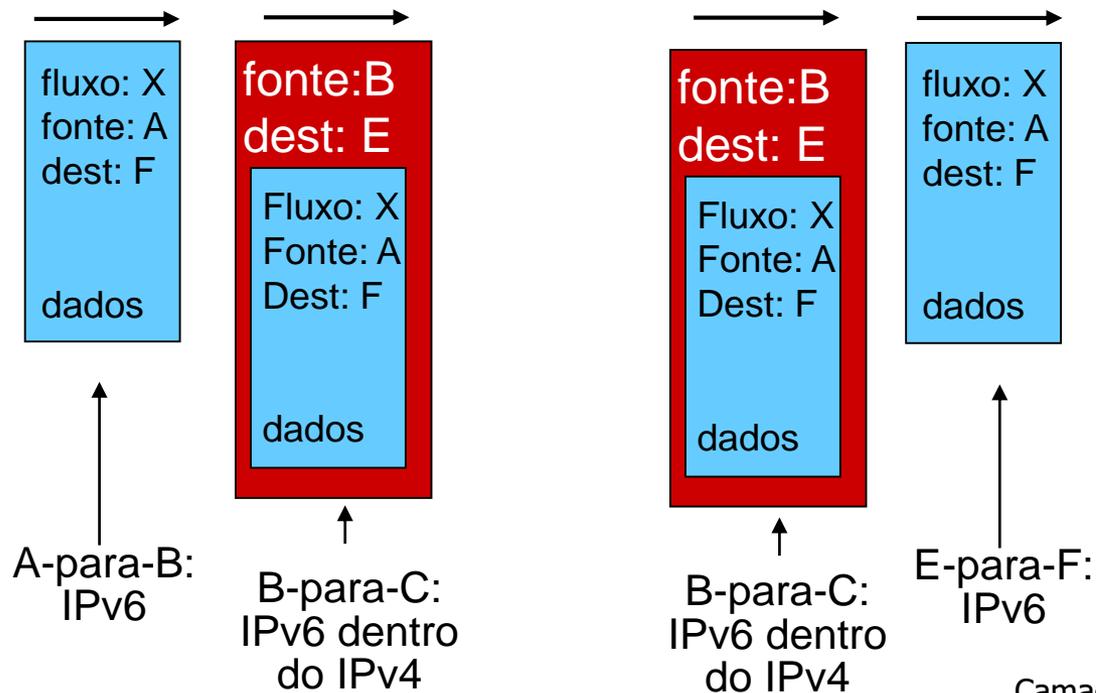
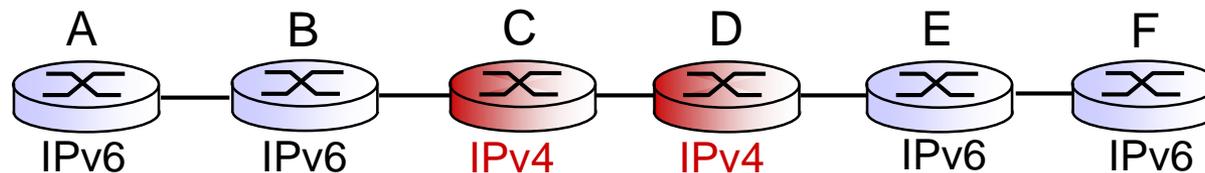


Tunelamento

visão lógica:



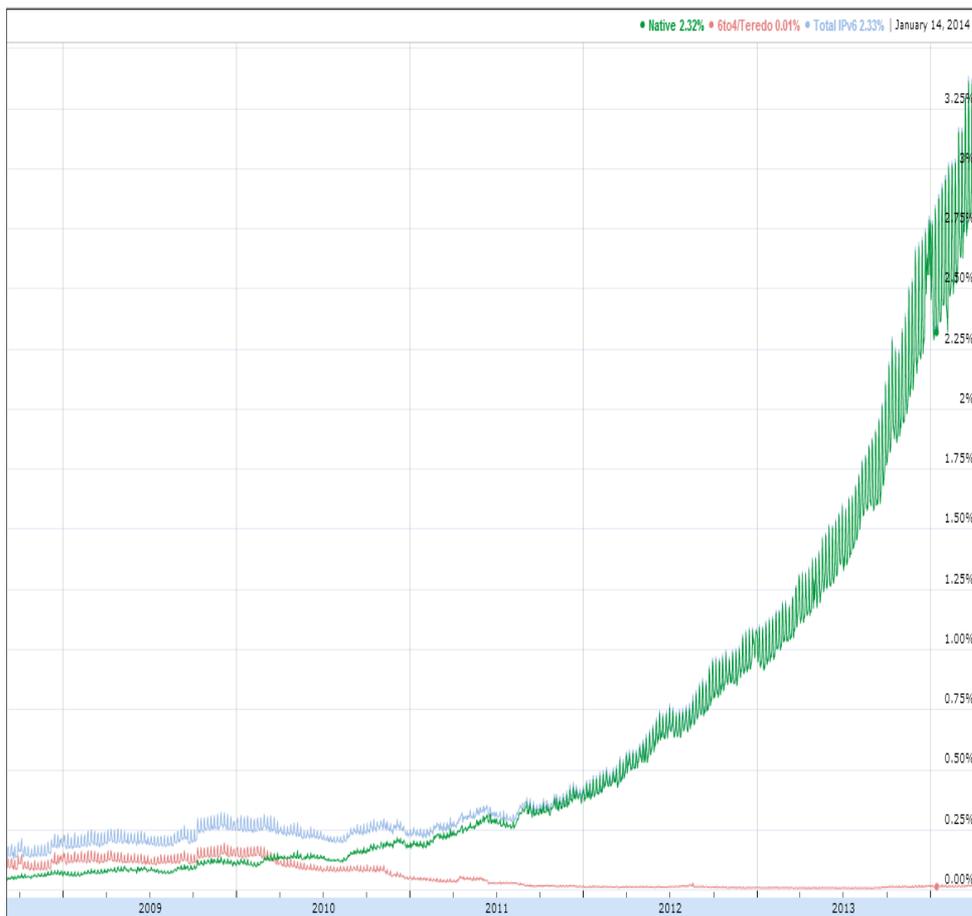
visão física:



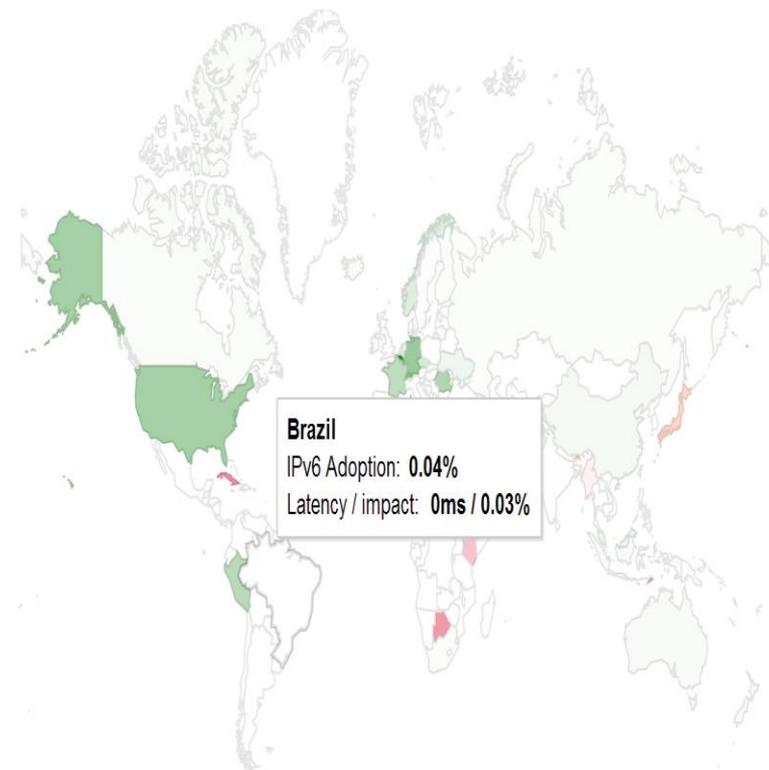
Estado em janeiro de 2014

Veja

- <http://ipv6.br/>
- <http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>



Per-Country IPv6 adoption

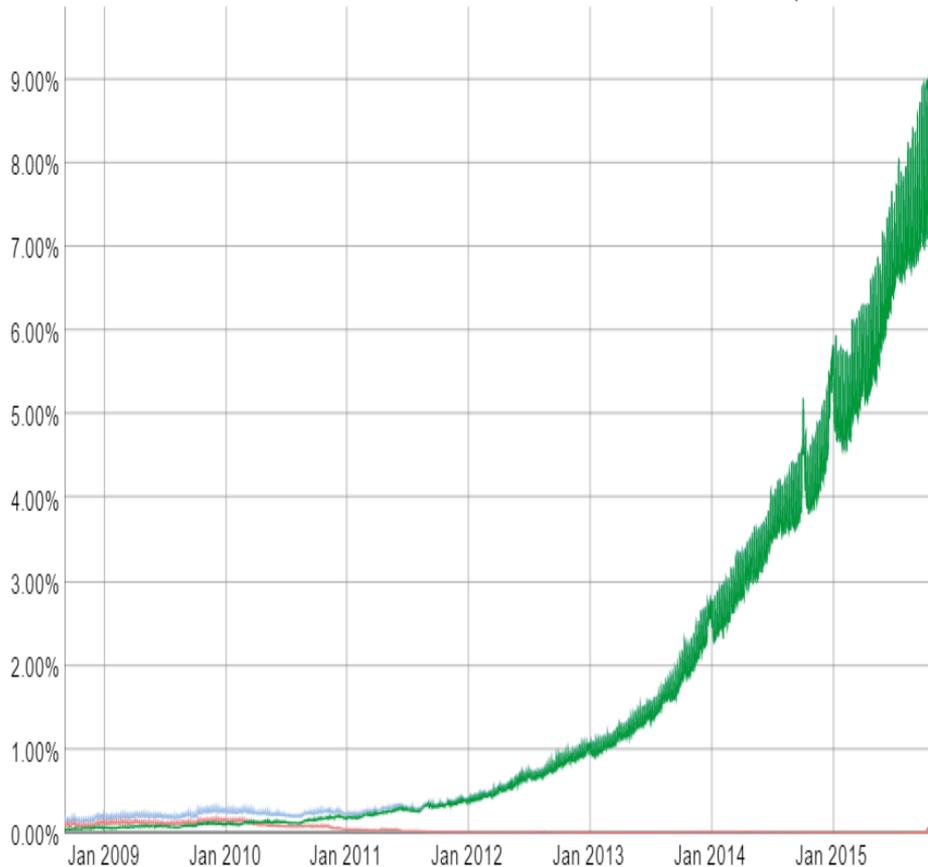


Estado em outubro 2015

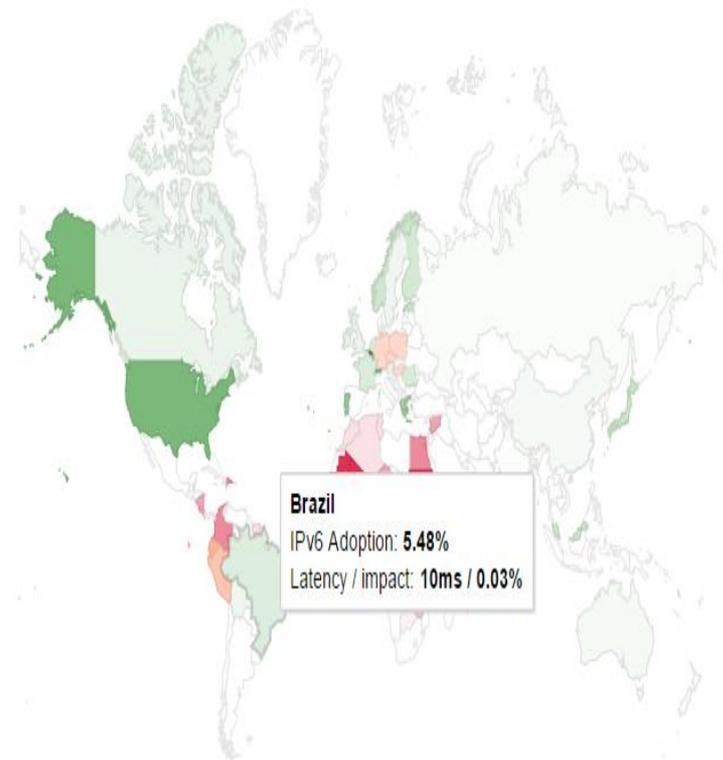
Veja

- <http://ipv6.br/>
- <http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>

Native: 8.94% 6to4/Teredo: 0.01% Total IPv6: 8.94% | 18 de out de 2015



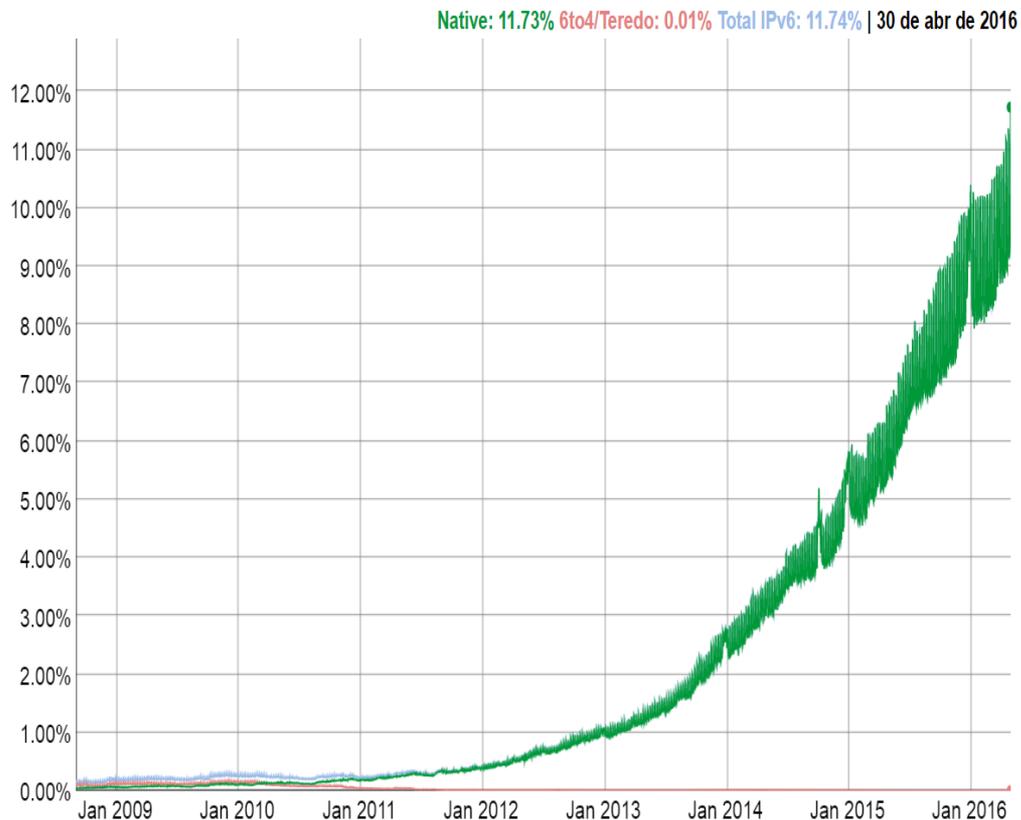
Per-Country IPv6 adoption



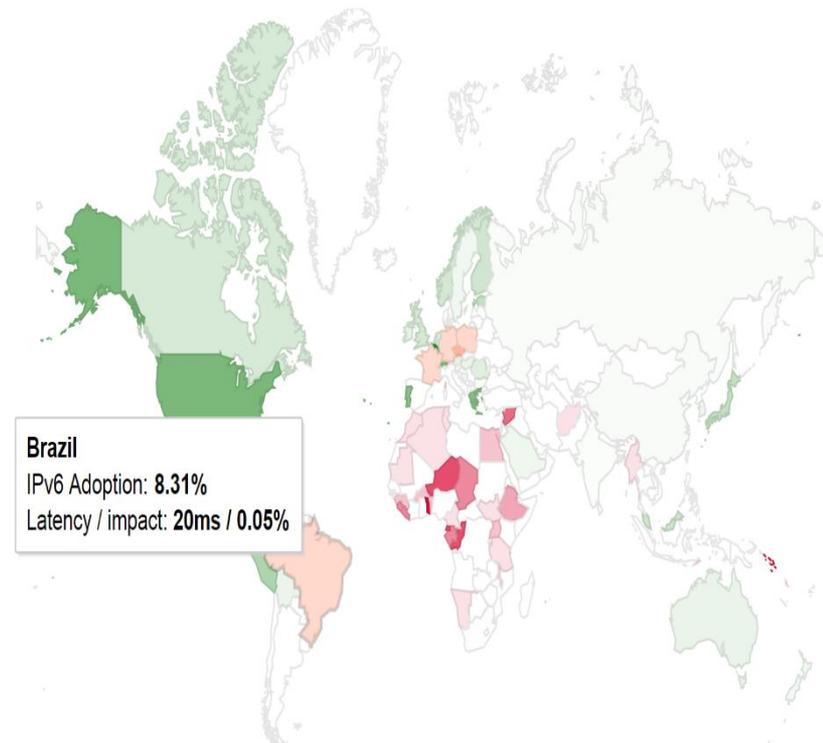
Estado atual: abril 2016

Veja

- <http://ipv6.br/>
- <http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>



Per-Country IPv6 adoption

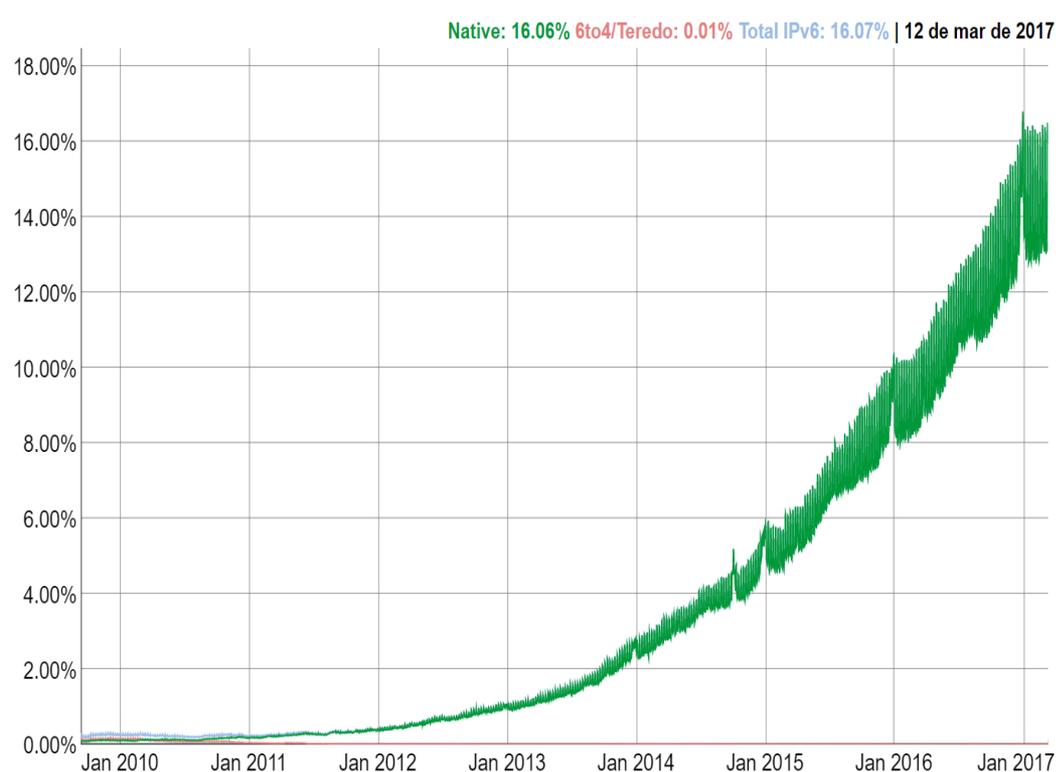


Estado atual: março 2017

Veja

- <http://ipv6.br/> - Teste sua conectividade IPv6
- <http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>

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



Per-Country IPv6 adoption

