

## A Camada de Rede

### Referências:

- Tanenbaum, A.; Wetherall, D., Redes de Computadores, 5ª edição, Pearson, 2011 - Capítulo 5
- Kurose, J.; Ross, K., Redes de Computadores e a Internet. Pearson, 2010 - Capítulo 4

## Objetivos do capítulo:

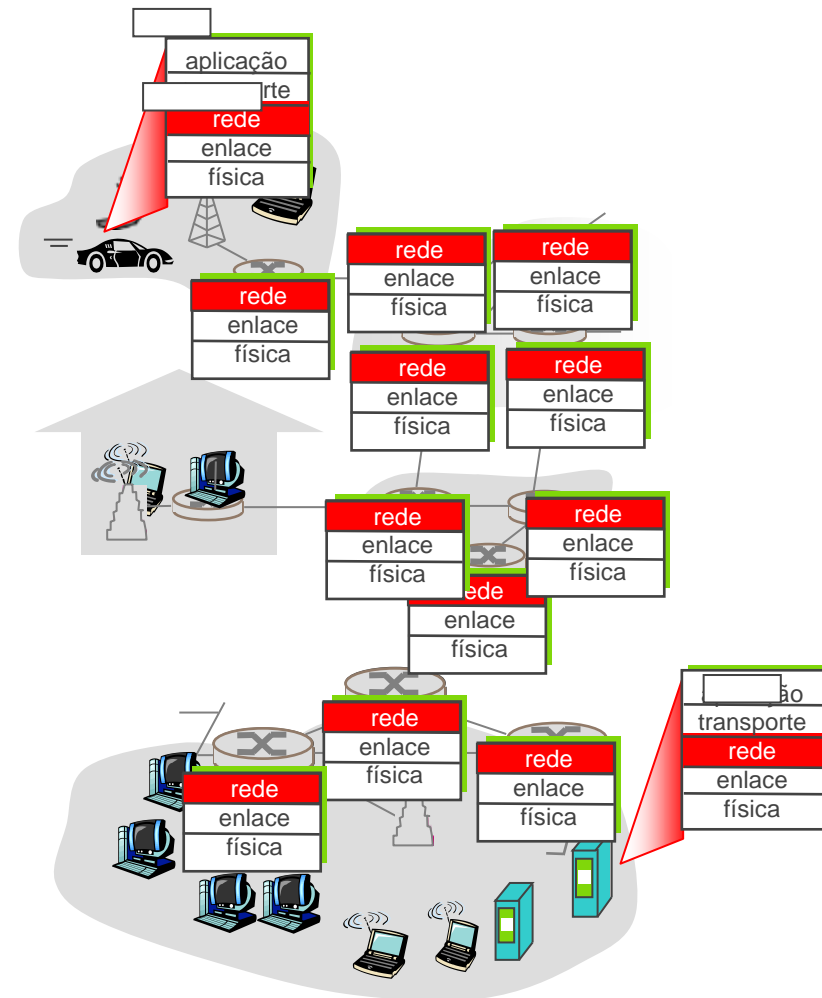
- **entender os princípios dos serviços da camada de rede:**
  - modelos de serviço da camada de rede
  - repasse *versus* roteamento
  - como funciona um roteador
  - roteamento (seleção de caminho)
  - lidando com escala
  - tópicos avançados: IPv6, mobilidade

- **4. 1 Introdução**
- **4.2 Redes de circuitos virtuais e de datagramas**
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

- Uma das camadas mais complexas da pilha de protocolos TCP/IP.
- Relacionada a transferência de pacotes da origem para o destino.
- Chegar ao destino pode exigir vários saltos (*hops*) em roteadores intermediários no percurso.
- Deve escolher os caminhos mais apropriados através do conjunto de roteadores da rede.
- Buscar rotas que evitem sobrecarregar algumas linhas de comunicação e roteadores enquanto deixam outras ociosas.

# Camada de rede

- **segmento de transporte do host** emissor ao receptor
- Lado emissor encapsula segmentos em datagramas;
- Protocolos da camada de rede em *cada* roteador;
- Roteador examina campos de cabeçalho em todos os datagramas IP que passam por ele;
- Datagrama chega ao receptor
- Datagrama é desencapsulado e entregue à camada de transporte;



# Duas importantes funções da camada de rede

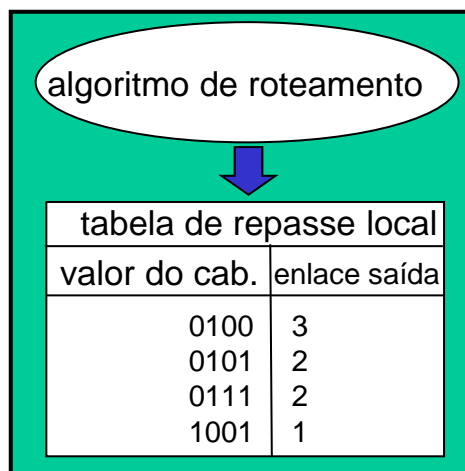


- **repasse:** mover pacotes da entrada do roteador para a saída apropriada do roteador
- **roteamento:** determinar rota seguida pelos pacotes da origem ao destino
  - *algoritmos de roteamento*

## analogia:

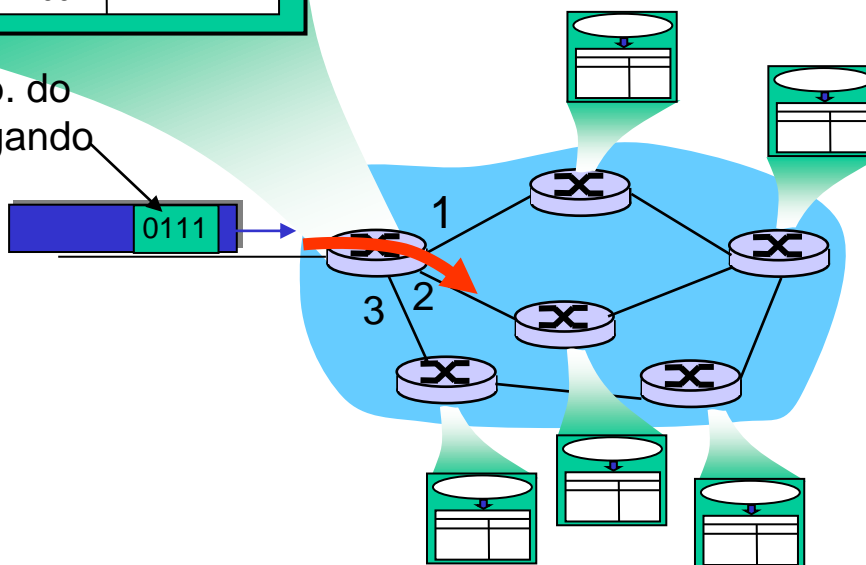
- **roteamento:** processo de planejamento da viagem da origem ao destino
- **repasse:** processo de passar por um único cruzamento

# Interação entre roteamento e repasse



- **Tabela de repasse:** indica qual das interfaces de enlace do roteador o pacote deve ser repassado.

valor no cab. do pacote chegando



- **Função importante em *algumas* arquiteturas de rede:**
  - ATM, MPLS, X.25
- **Antes que os datagramas fluam, 2 hosts finais e roteadores entre eles estabelecem conexão virtual;**
  - roteadores são envolvidos
- **serviço de conexão da **camada de rede** vs **transporte**:**
  - **rede:** entre dois hospedeiros (também pode envolver roteadores entre eles, no caso de VCs), providos à camada de transporte;
  - **transporte:** entre dois processos, fornecidos à camada de aplicação



Diferentes tipos de serviços podem ser oferecidos pela camada de rede:

**P: Que *modelo de serviço* é o melhor para o “canal” que transporta datagramas do remetente ao destinatário?**

- **Entrega garantida:** Assegura que o pacote mais cedo ou mais tarde, chegará ao seu destino;
- **Entrega garantida com atraso limitado:** Assegura a entrega, com um atraso host a host limitado e especificado (ex. até 100 ms);
- **Entrega de datagrama na ordem:** Garante ordenamento dos pacotes;
- **Largura de banda mínima garantida:** Emula o comportamento de um enlace com taxa de bits especificada (ex. 50 Mbps) entre hosts remetentes e destinatários. (mesmo que o caminho fim a fim passe por vários enlaces)

Diferentes tipos de serviços podem ser oferecidos pela camada de rede:

- **Jitter máximo garantido:** Assegura que o tempo entre a transmissão de 2 pacotes sucessivos no remetente seja igual à quantidade de tempo de recebimento.
- **A camada de rede da Internet fornece um único modelo de serviço:**

## Serviço de melhor esforço:

- Não há garantia de temporização entre pacotes
- Não há garantia de entrega
- Sem ordenação
- **Então a camada de rede da Internet não faz nada??**
- Existem razões sólidas para esse modelo minimalista de serviço de camada de rede.

- **A arquitetura de rede ATM habilita vários modelos de serviço:**
  - Dentro da mesma rede, podem ser oferecidas conexões diferentes com classe de serviço distintas.

Arquitetura da rede	Modelo de serviço	Garantia de largura de banda	Garantia contra perda	Ordenamento	Temporização	Indicação de congestionamento
Internet	Melhor esforço	Nenhuma	Nenhuma	Qualquer ordem possível	Não mantida	Nenhuma
ATM	CBR	Taxa constante garantida	Sim	Na ordem	Mantida	Não ocorrerá congestionamento
ATM	ABR	Mínima garantida	Nenhuma	Na ordem	Não mantida	Indicação de congestionamento

- 4. 1 Introdução
- **4.2 Redes de circuitos virtuais e de datagramas**
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

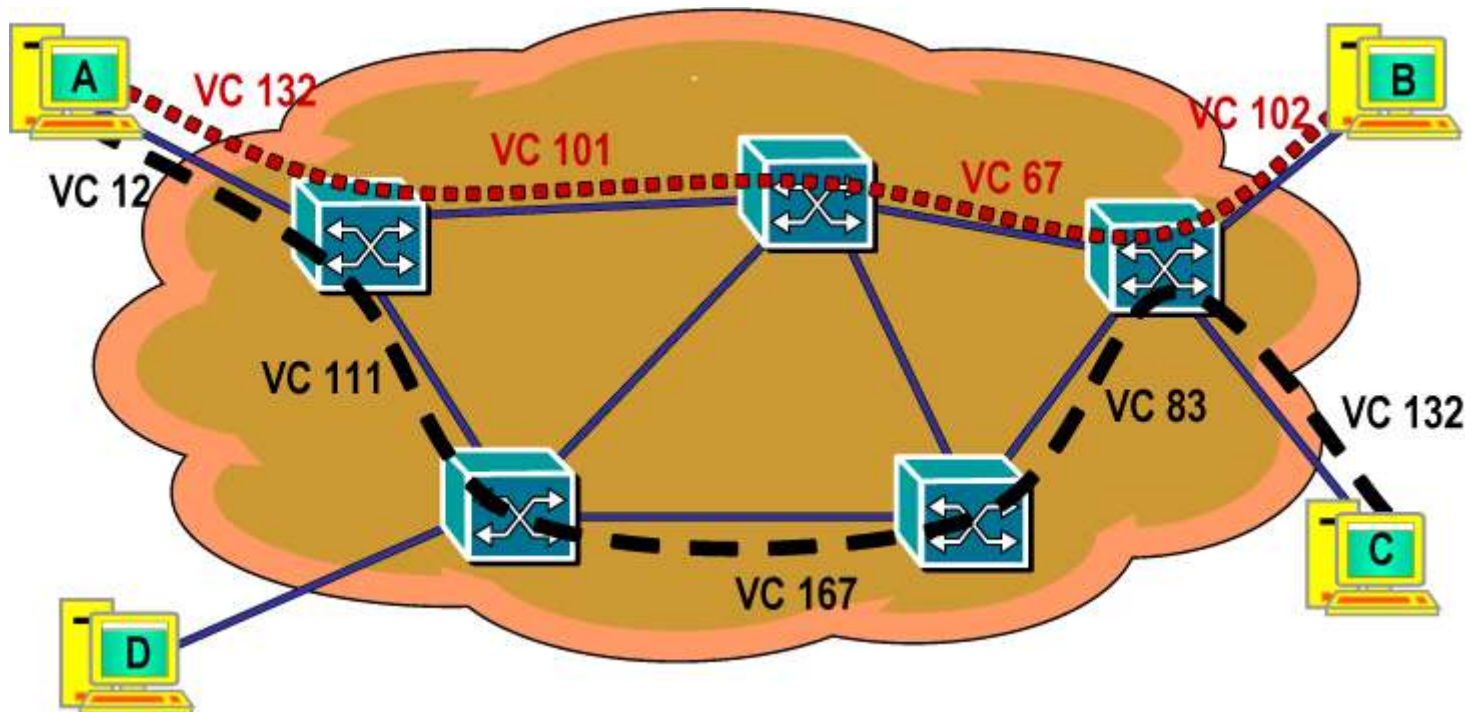
- Rede de datagrama fornece serviço sem conexão;
- Rede de Circuito Virtual fornece serviço com conexão;
- Análogo aos serviços da camada de transporte:
  - Protocolos TCP e UDP;
- Porém:
  - **serviço:**
    - **Camada de rede:** hospedeiro a hospedeiro
    - **Camada de transporte:** processo a processo
  - **sem escolha:** a rede oferece um ou outro!
  - **implementação:**
    - **Cam. rede:** no núcleo da rede
    - **Cam. transporte:** no host

## **“Caminho da origem ao destino comporta-se como um circuito telefônico”**

- com respeito ao desempenho
  - ações da rede ao longo do caminho da origem ao destino
- 
- *estabelecimento e término para cada chamada antes que os dados possam fluir;*
  - *cada pacote carrega identificador VC (não endereço do hospedeiro de destino);*
  - *cada roteador no caminho origem-destino mantém “estado” para cada conexão que estiver passando;*
  - *recursos do enlace e roteador (largura de banda, buffers) podem ser alocados ao VC (recursos dedicados = serviço previsível);*

# Circuitos virtuais

**Circuito virtual:** rota para os pacotes é estabelecida a priori.  
Estabelecido o VC, todos os pacotes seguem pela mesma rota.  
Cada um carrega informação de qual VC tomar em cada roteador.



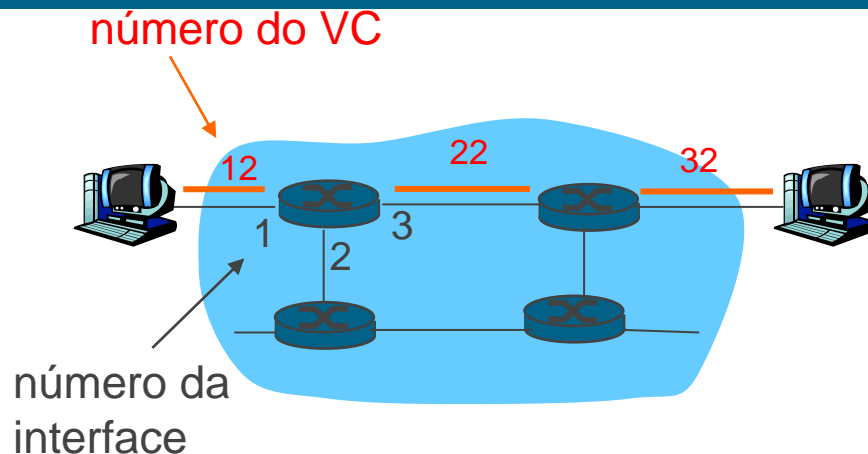
**um VC consiste em:**

1. caminho da origem ao destino
  2. números de VC, um número para cada enlace ao longo do caminho
  3. entradas em tabelas de repasse nos roteadores ao longo do caminho
- pacote pertencente ao VC carrega número do VC (em vez do endereço de destino)
  - número do VC pode ser alterado em cada enlace
    - novo número de VC vem da tabela de repasse



# Tabela de repasse

tabela de repasse no roteador noroeste:

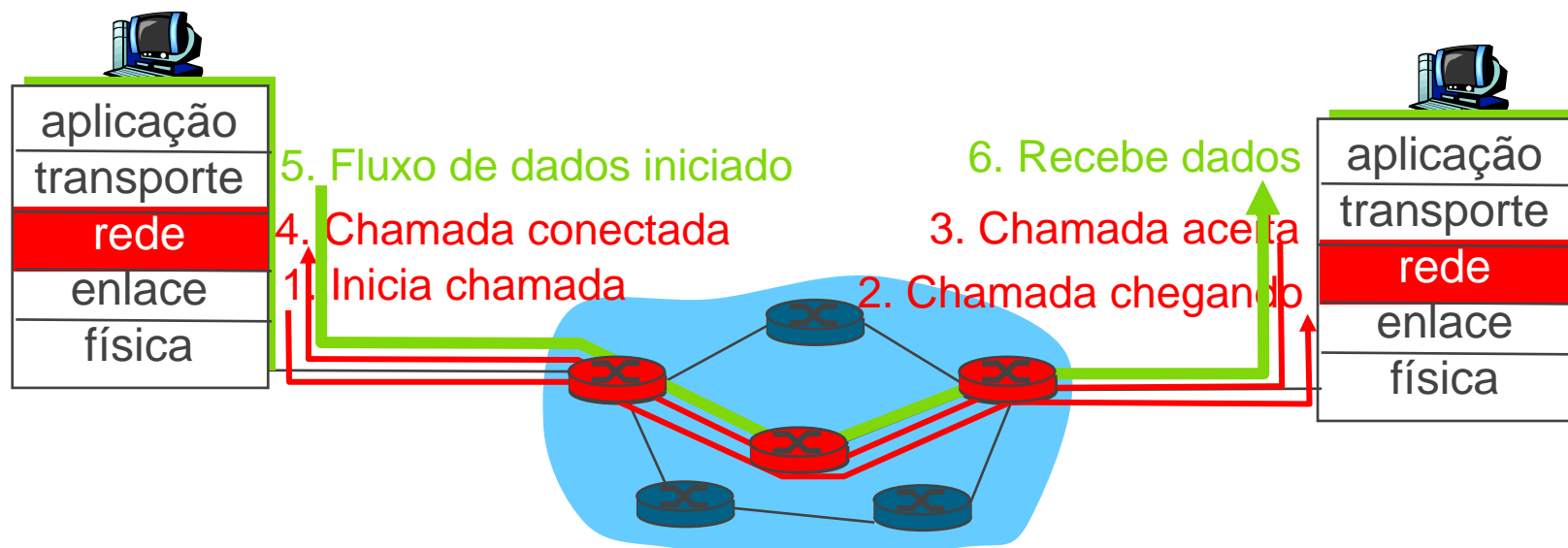


Interface de entrada	Nº do CV de entrada	Interface de saída	Nº do CV de saída
1	12	2	22
2	63	1	18
3	7	2	17
1	97	3	87
...	...	...	...

Roteadores mantêm informação de estado da conexão!

# Circuitos virtuais: protocolos de sinalização

- usados para estabelecer, manter e terminar VC
- usados em ATM, MPLS, frame-relay, X.25
- O uso destas redes estão em declínio



## Benefícios dos Circuitos Virtuais:

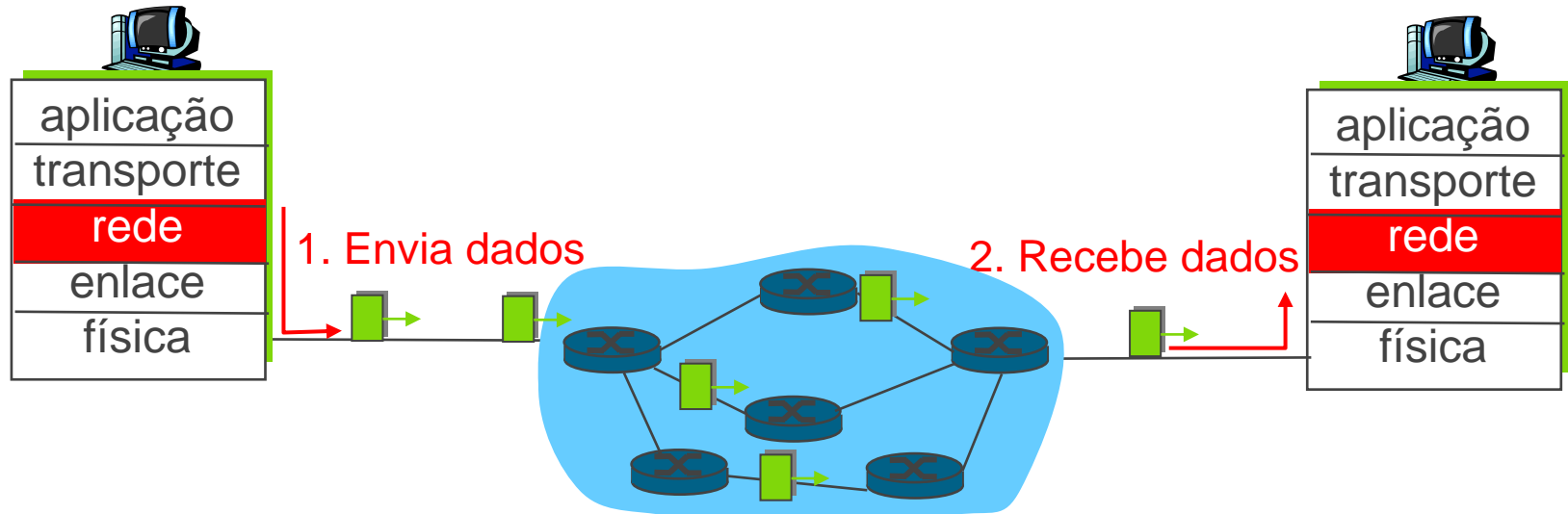
- Previsibilidade e desempenho:
  - Tráfego é mais previsível;
  - Desempenho pouco afetado em situações de gargalos na Internet.
- Qualidade de Serviço (QoS):
  - possível garantir níveis de BW, latência, jitter, perda de pacotes;
  - ideal para aplicações que exigem alta confiabilidade.
- Transferência de dados confiável:
  - VC podem garantir a entrega dos pacotes, melhora a qualidade geral da transmissão de dados.
- Baixa Sobrecarga de Roteamento:
  - Após estabelecer o VC, o encaminhamento de pacotes requer menos processamento.

## Limitações dos Circuitos Virtuais:

- Subutilização de recursos:
  - A reserva de recursos (como BW) levar a subutilização, especialmente se o tráfego de dados for intermite.
- Custo:
  - São redes mais caras que as de Datagrama.
- Flexibilidade limitada:
  - São incapazes de se adaptar a condições de rede em mudança, o que pode afetar potencialmente o desempenho.
- Tempo de configuração:
  - Em caso de falha em algum ponto, todo o VC deve ser reconfigurado, o que pode causar interrupções/atrasos no serviço;

# Redes de datagrama

- **sem estabelecimento de estabelecimento de conexão ou circuito virtual.**
- **roteadores:** sem estado sobre conexões fim a fim (não existe conexão)
- **pacotes são encaminhados com base no endereço de destino**
  - Na Internet, o end. IP será usado para a definir a rota.
  - pacotes entre mesmo par origem-destino podem tomar caminhos diferentes



# Tabela de repasse

4 bilhões de entradas  
possíveis

## Faixa de endereços de destino

## Interface de enlace

11001000 00010111 00010000 00000000  
até

0

11001000 00010111 00010111 11111111

11001000 00010111 00011000 00000000  
até

1

11001000 00010111 00011000 11111111

11001000 00010111 00011001 00000000  
até

2

11001000 00010111 00011111 11111111

senão

3

# Concordância do prefixo mais longo

- Seria impraticável manter um registro para cada endereço de destino...
  - Não é necessário ter 4 bilhões de registros na tabela do roteador. Neste caso apenas 4 seriam suficientes!

**Roteador compara um prefixo do endereço de destino com registros em sua tabela.**

Concordância do prefixo	Interface do 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?

## Internet (datagrama)

- **troca de dados entre computadores**
  - serviço “elástico”, sem requisitos de temporização estritos ;
- **sistemas finais “inteligentes” (computadores)**
  - pode adaptar, realizar controle, recup. de erros;
  - simples dentro da rede, complexidade na “borda”;
- **muitos tipos de enlace**
  - diferentes características
  - serviço uniforme difícil;

## MPLS (VC)

- **evoluída da telefonia**
- **conversação humana:**
  - requisitos de temporização estritos, confiabilidade;
  - necessário para serviço garantido;
- **sistemas finais “burros”**
  - telefones;
  - complexidade dentro da rede;



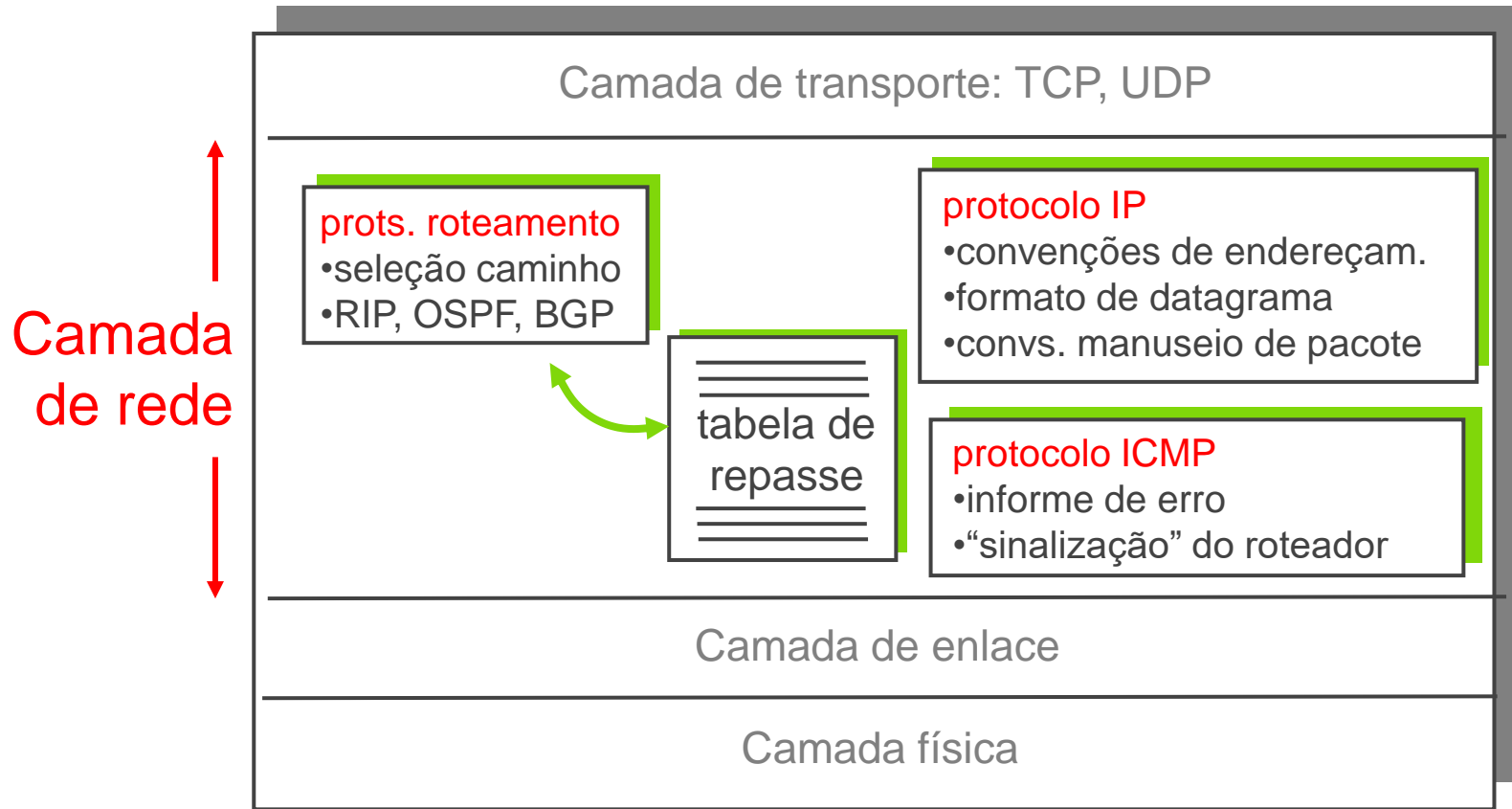
# Rede de datagramas ou VC: por quê?

<b>Questão</b>	<b>Sub-rede de datagramas</b>	<b>Sub-rede de circuitos virtuais</b>
Configuração de circuitos	Desnecessária	Obrigatória
Endereçamento	Cada pacote contém os endereços de origem e de destino completos	Cada pacote contém um número de circuito virtual curto
Informações sobre o estado	Os roteadores não armazenam informações sobre o estado das conexões	Cada circuito virtual requer espaço em tabelas de roteadores por conexão
Roteamento	Cada pacote é roteado independentemente	A rota é escolhida quando o circuito virtual é estabelecido; todos os pacotes seguem essa rota
Efeito de falhas no roteador	Nenhum, com exceção dos pacotes perdidos durante a falha	Todos os circuitos virtuais que tiverem passado pelo roteador que apresentou o defeito serão encerrados
Qualidade de serviço	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual
Controle de congestionamento	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual

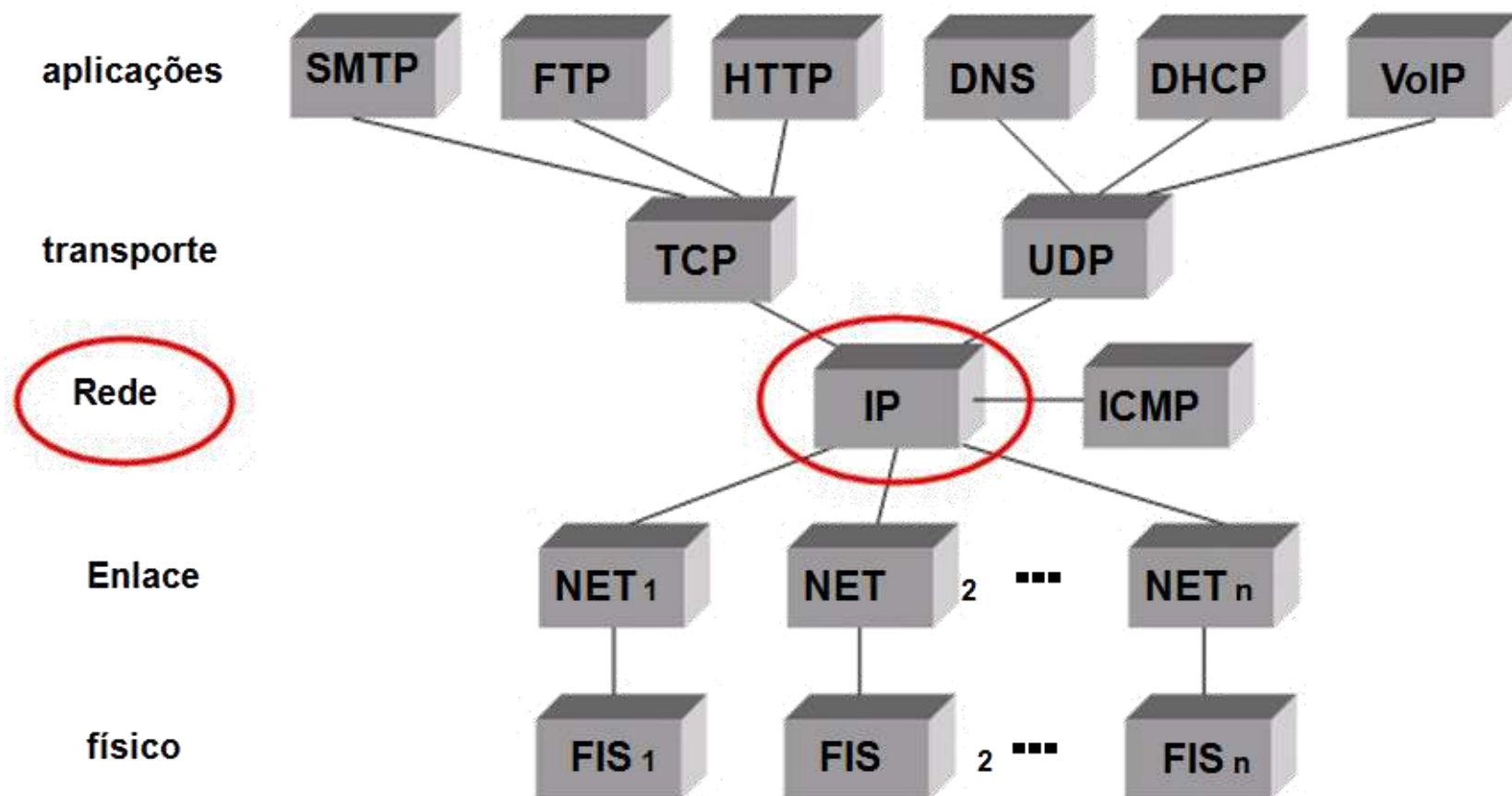
- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

# A camada de rede da Internet

## Funções na camada de rede do hospedeiro e roteador:

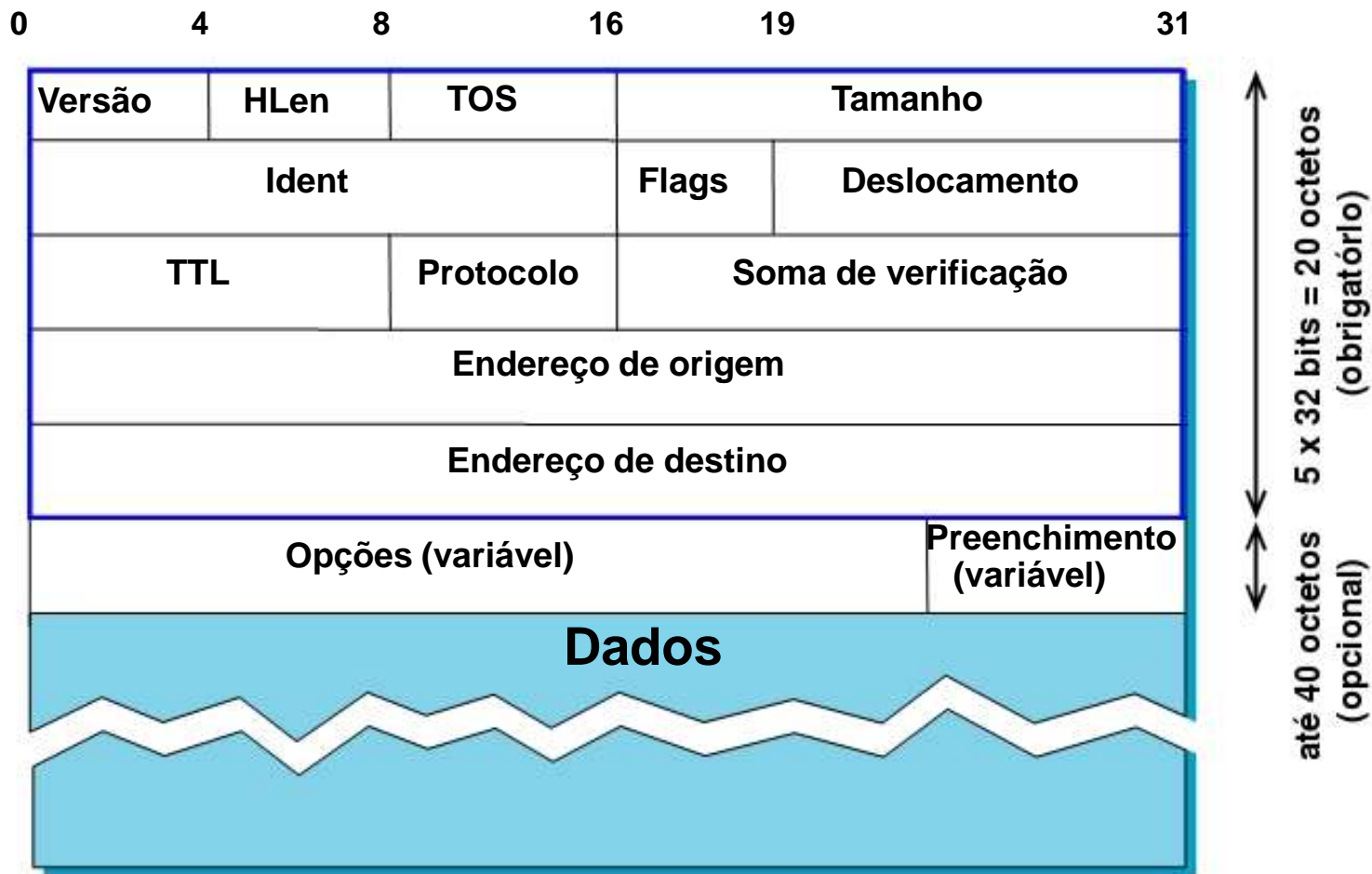


# A camada de rede e Encapsulamento

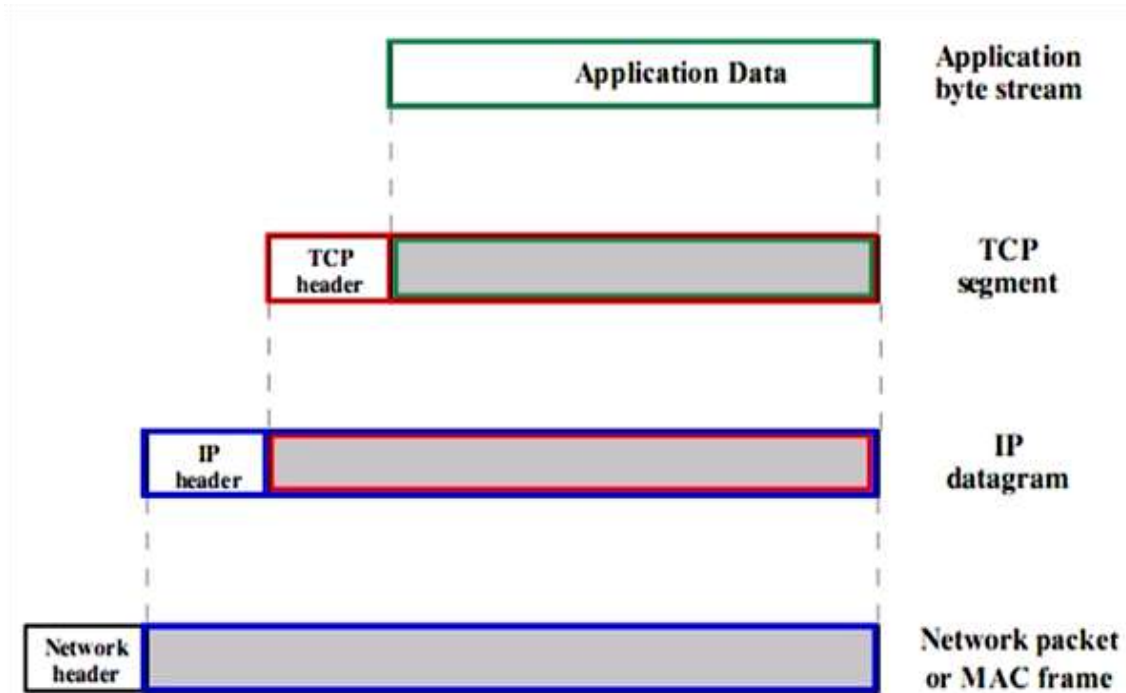


- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

# Formato do datagrama IP



# Formato do datagrama IP

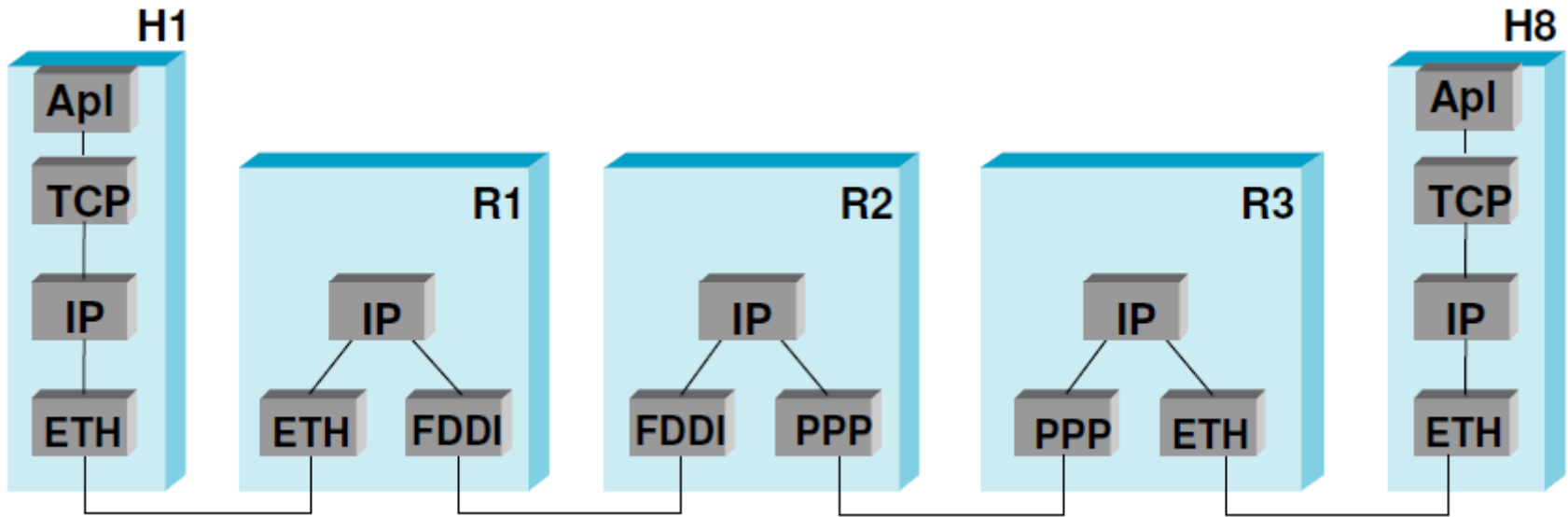


Quanto overhead com TCP?

- ❑ 20 bytes de TCP
- ❑ 20 bytes de IP
- ❑ = 40 bytes + overhead da camada de aplicação

# Inter-rede baseada em IP

- O IP é a ferramenta para montar redes escaláveis e heterogêneas.
- Hosts H1 e H8 estão conectados logicamente pela inter-rede abaixo.



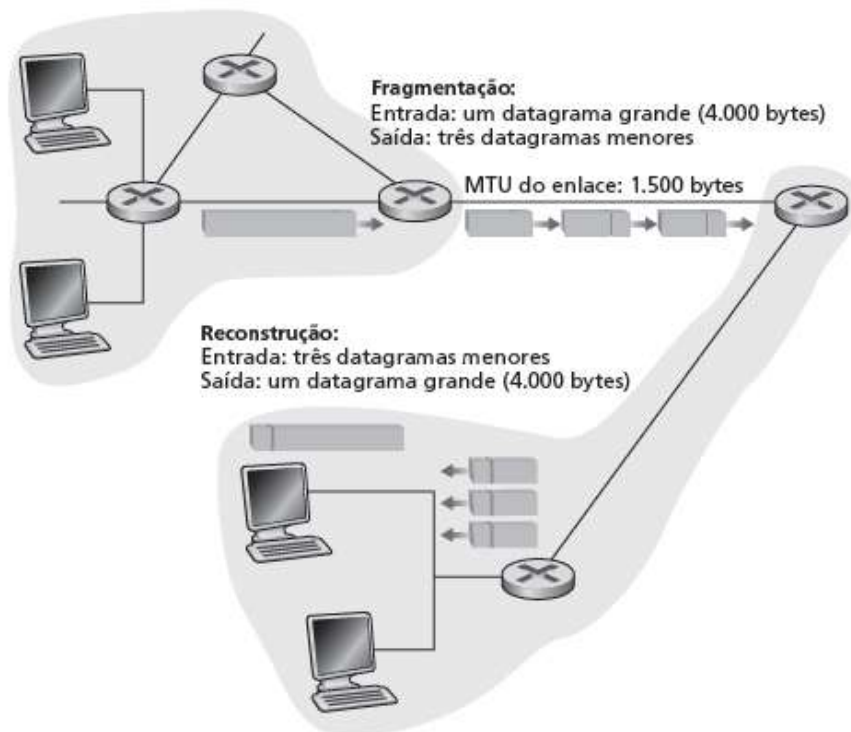
- Os protocolos TCP e UDP e as aplicações são executados nos hosts, em cima do IP.



- Problema em se oferecer um modelo de serviço para redes heterogêneas é que cada tecnologia de rede suporta um tamanho de pacote diferente.
  - Ex: Ethernet: 1500 bytes, FDDI: 4500 bytes
- 2 opções para o modelo de serviço IP:
  - certificar que todos datagramas sejam pequenos o suficiente para trafegar em qualquer tipo de rede;
  - oferecer um meio para que os pacotes sejam fragmentados e remontados quando forem grandes para seguir em determinadas redes.
- Porém, novas tecnologias surgiram e...
- Limitar o tamanho dos pacotes poderia consumir largura de banda e consumiria recursos de processamento, além de um orverhead extra...

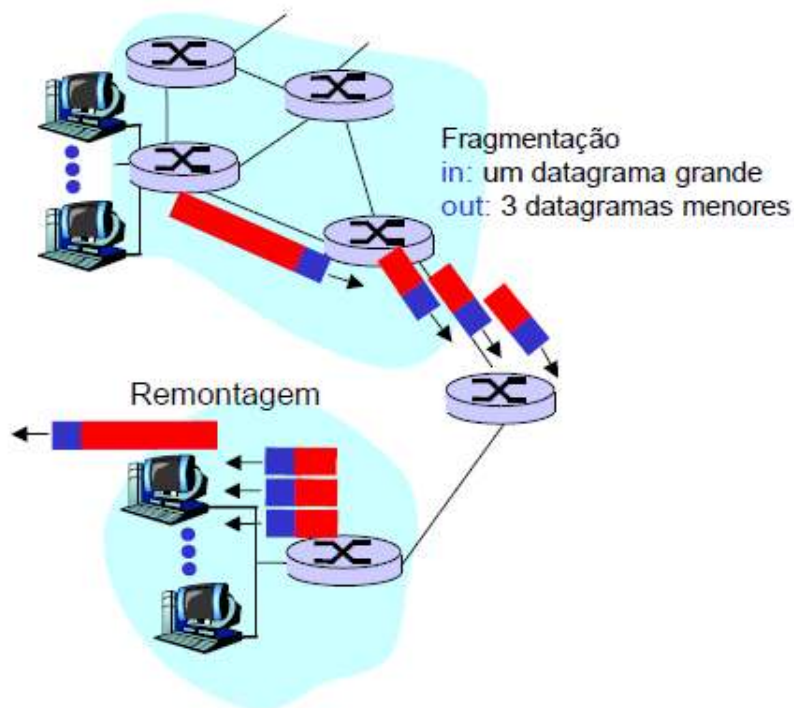
# Fragmentação e reconstrução do IP

- **enlaces de rede têm MTU** (tamanho máx. transferência) – **maior quadro em nível de enlace possível.**
  - diferentes tipos de enlace, diferentes MTUs
- **grande datagrama IP dividido (“fragmentado”) dentro da rede**
  - um datagrama torna-se vários datagramas
  - “reconstruído” somente no destino final
  - bits de cabeçalho IP usados para identificar, ordenar fragmentos relacionados



# Fragmentação e reconstrução do IP

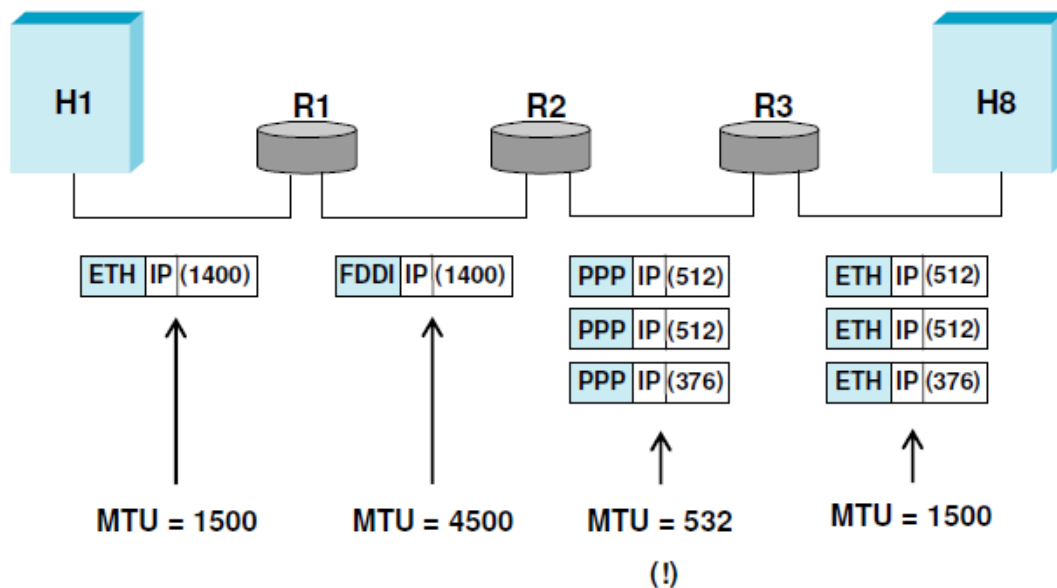
- A fragmentação ocorre nos roteadores.
- A remontagem dos pacotes ocorre só no **destino**.



- Para permitir que os fragmentos sejam remontados, todos datagramas carregam um identificador no campo *Ident*.

# Fragmentação e reconstrução do IP

- Host 1 envia um datagrama para o host 8 na rede.
- Datagrama precisa ser fragmentado no R2 para ser encaminhado ao H8.
  - MTU 532 bytes = 20 (header) + 512 (data).



Início do cabeçalho			
Ident = x		0	Desloc. = 0
Restante do cabeçalho			
1400 bytes de dados			



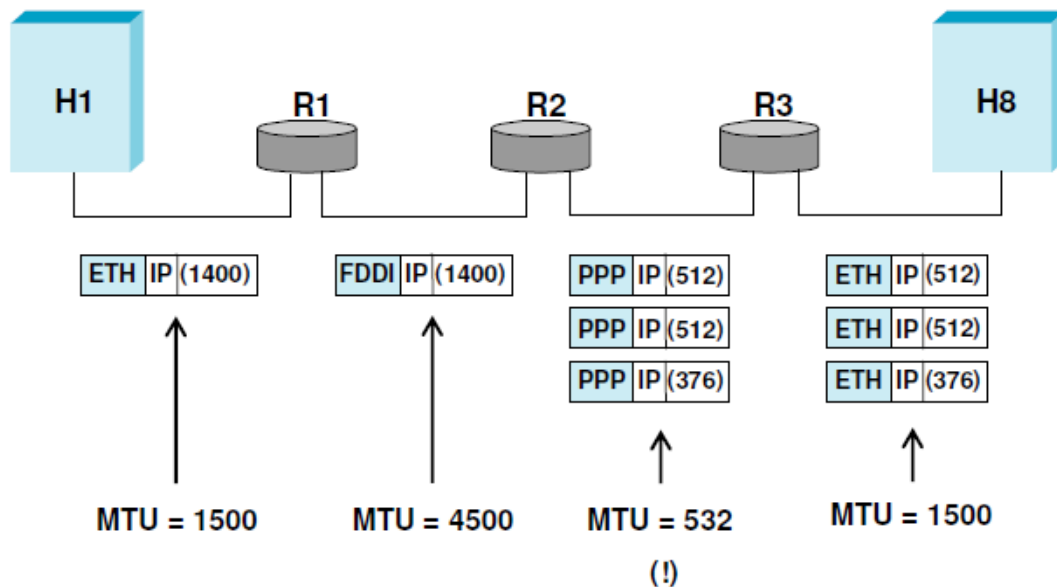
Início do cabeçalho			
Ident = x		1	Desloc. = 0
Restante do cabeçalho			
512 bytes de dados			

Início do cabeçalho			
Ident = x		1	Desloc. = 64
Restante do cabeçalho			
512 bytes de dados			

Início do cabeçalho			
Ident = x		0	Desloc. = 128
Restante do cabeçalho			
376 bytes de dados			

# Fragmentação e reconstrução do IP

- R2 marca o bit M do campo *flags*, indicando que há mais fragmentos a seguir;
- Define o *Offset*=0, pois esse fragmento contém a primeira parte do datagrama original;
- Dados do 2º fragmento iniciam com o 513º dos dados originais;
- Campo *Offset* = 64 (512 / 8 – múltiplos de 8 bytes).



Início do cabeçalho			
Ident = x		0	Desloc. = 0
Restante do cabeçalho			
1400 bytes de dados			



Início do cabeçalho			
Ident = x		1	Desloc. = 0
Restante do cabeçalho			
512 bytes de dados			

Início do cabeçalho			
Ident = x		1	Desloc. = 64
Restante do cabeçalho			
512 bytes de dados			

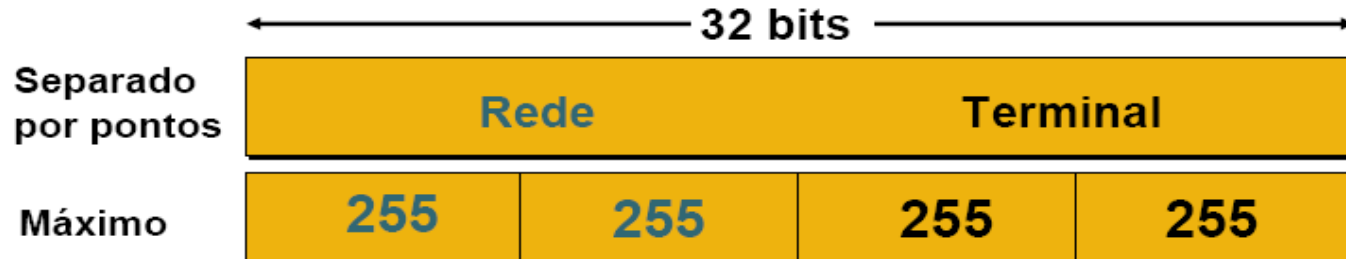
Início do cabeçalho			
Ident = x		0	Desloc. = 128
Restante do cabeçalho			
376 bytes de dados			

- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - **endereço IPv4**
  - ICMP
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

- O IP é um **endereço lógico** único em toda a rede.
  - Quando estamos acessando a Internet, utiliza-se um endereço IP único mundialmente, pois a Internet é uma rede global.
  - Em LANs pode-se utilizar endereços não válidos para navegação.
  - No entanto, cada máquina da LAN utilizará um único IP nesta rede local.
- Um endereço IP está **associado com uma interface**, e não com um host ou roteador que contém aquela interface.
- Um endereço IP consiste em 4 bytes ou 32 bits.
  - É comum a segmentação dos 32 bits do IP em quatro octetos.
  - Este formato é chamado notação decimal pontuada.
  - Ex: 200.192.45.12

# Endereçamento IPv4

- Cada endereço IP inclui uma identificação de rede e host (máquina)
  - O **endereço de rede** identifica os sistemas que estão localizados no mesmo segmento físico de rede na abrangência de roteadores IPs.
  - A identificação de rede deve ser única na rede.
  - O endereço de host identifica um computador, servidor ou roteador dentro da rede.

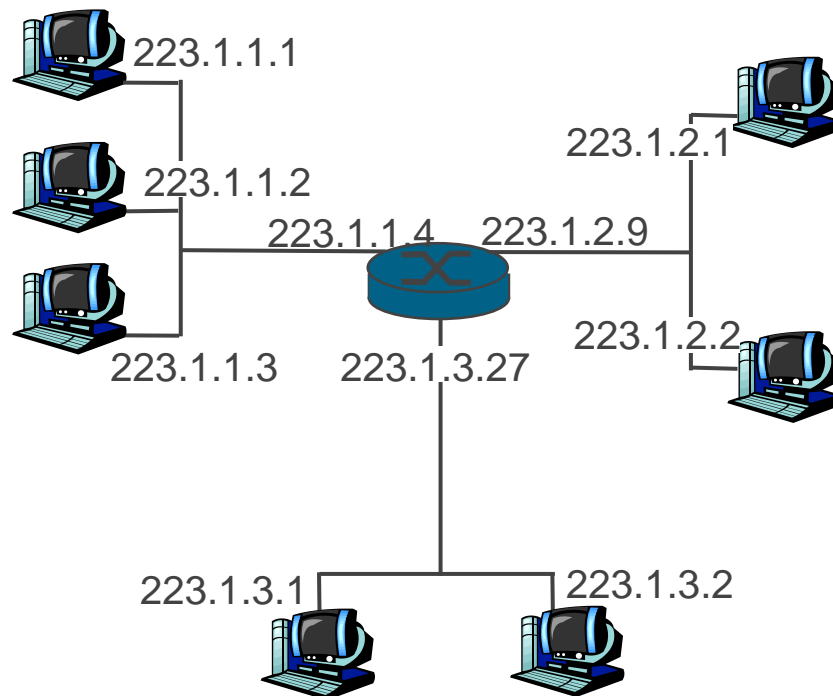


	Endereço decimal	Binário
Endereço completo	192.168.5.10	11000000.10101000.00000101.00001010
Máscara da subrede	255.255.255.0	11111111.11111111.11111111.00000000
Porção da rede	192.168.5.0	11000000.10101000.00000101.00000000



# Endereçamento IP: introdução

- **endereço IP:** identificador de 32 bits para *interface de* hospedeiro e roteador
- **interface:** conexão entre hospedeiro/ roteador e enlace físico
  - roteadores normalmente têm várias interfaces
  - hospedeiro normalmente tem uma interface
  - endereços IP associados a cada interface



$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{1}$$

# Endereçamento IPv4: classes

- Existiam 5 classes (A,B,C,D,E) de endereços IP, que variavam conforme a quantidade de endereços de rede existente.
- O objetivos das classes:
  - determinar qual parte do endereço IP pertence a rede e ao host,
  - permitir que uma melhor distribuição dos endereços IPs.

	8 bits	8 bits	8 bits	8 bits
• <b>Classe A:</b>	Rede	Terminal	Terminal	Terminal
• <b>Classe B:</b>	Rede	Rede	Terminal	Terminal
• <b>Classe C:</b>	Rede	Rede	Rede	Terminal
• <b>Classe D:</b>	Multicast			
• <b>Classe E:</b>	Pesquisa			

# Endereçamento IPv4: classes

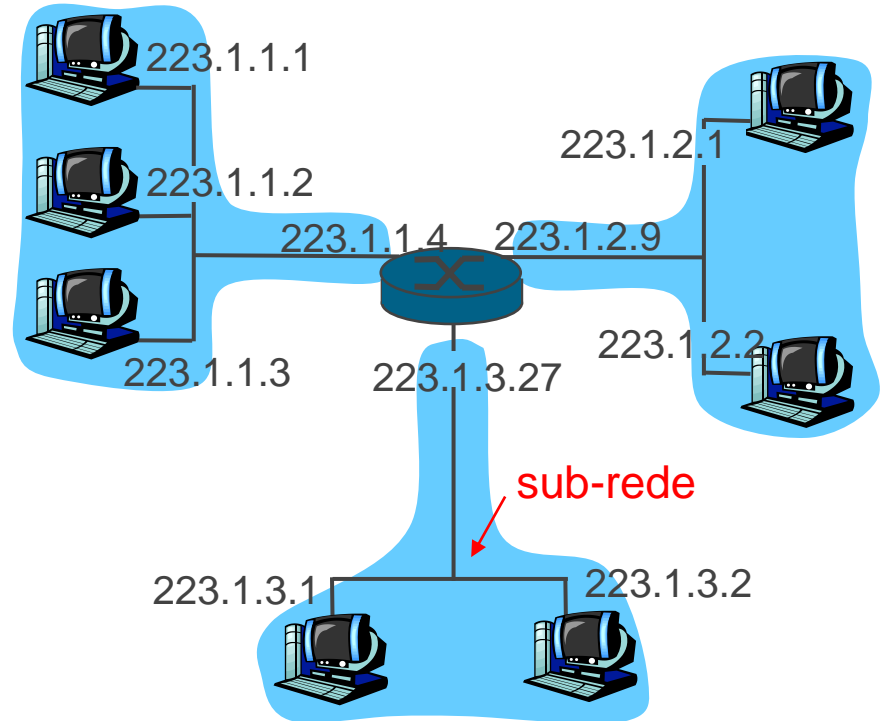
- **Classe A:** três primeiros números identificam a rede e os últimos números identificam o próprio host.
  - 1º byte do endereço está entre 1 e 126.
  - Ex: 13.0.0.1 - 80.10.69.12 - 37.25.10.99
- **Classe B:** dois primeiros octetos identificam a rede e os outros dois números identificam o host.
  - 1º byte do endereço está entre 128 e 191.
  - Ex: 133.0.0.1 - 140.10.69.12 - 190.25.10.99.

	8 bits	8 bits	8 bits	8 bits
• Classe A:	Rede	Terminal	Terminal	Terminal
• Classe B:	Rede	Rede	Terminal	Terminal
• Classe C:	Rede	Rede	Rede	Terminal
• Classe D:	Multicast			
• Classe E:	Pesquisa			

- **Classe C:** primeiro octeto identifica a rede e os outros três números identificam o próprio host.
  - 1º byte do endereço está entre 192 e 223.
  - Ex: 200.0.0.1 - 220.10.69.12 - 195.25.10.99
- **Classe D:** classe reservada para criar agrupamentos de hosts para o uso de Multicast.
- Não utilizada para endereçar hosts na rede TCP/IP.
  - 1º byte do endereço está entre 224 e 239.
  - Ex: 225.0.0.1 - 239.10.69.12 - 226.25.10.99
- **Classe E:** reservada para testes e novas implementações.
- Não utilizada para endereçar os computadores na rede TCP/IP.
  - 1º byte do endereço está acima de 240.

- **Endereço da rede**
  - 200.220.150.0    ou    192.168.7.0    -    ....
- **Endereços de broadcast**
  - 255.255.255.255    ou    192.168.7.255
- **Endereços de loopback**
  - 127.0.0.1
- **Endereços privados utilizados em LANs (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

- **endereço IP:**
  - parte da sub-rede (bits de alta ordem)
  - parte do host (bits de baixa ordem)
- ***O que é uma sub-rede?***
  - dispositivo se conecta à mesma parte da sub-rede do endereço IP
  - pode alcançar um ao outro fisicamente sem roteador intermediário



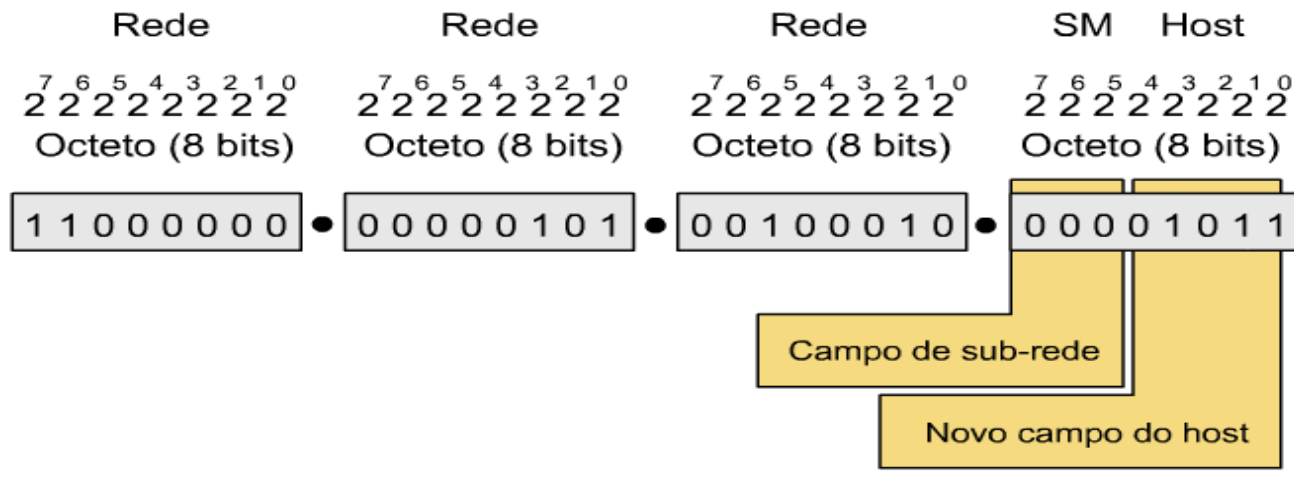
rede consistindo em 3 sub-redes

- Existem casos que é necessário subdividir uma rede em redes menores.
  - Imagine o administrador de uma rede classe A administrando 16,8 milhões de hosts?
  - Empresa com 600 estações de trabalho. Um endereço classe B seria um enorme desperdício...
  - Pequena empresa com 5 computadores...
- 2 nomenclaturas: **máscara de sub-rede e CIDR**
- A máscara de rede foi criada para formar sub-redes menores, e também possibilitar uma utilização mais eficiente dos IP disponíveis.
  - Máscara de Sub-rede serve para confirmar ou alterar o funcionamento das Classes de endereços padrões do TCP/IP.

# Sub-redes

Para criar um endereço de sub-rede, tomam-se “emprestados” bits do campo do host e os designa como o campo da sub-rede.

O máximo de bits que podem ser emprestados é qualquer número de bits que deixe pelo menos 2 bits para o número do host.





# Máscara de Sub-redes

Núm. de end. IP dentro de cada sub-rede =  $2^n - 2$

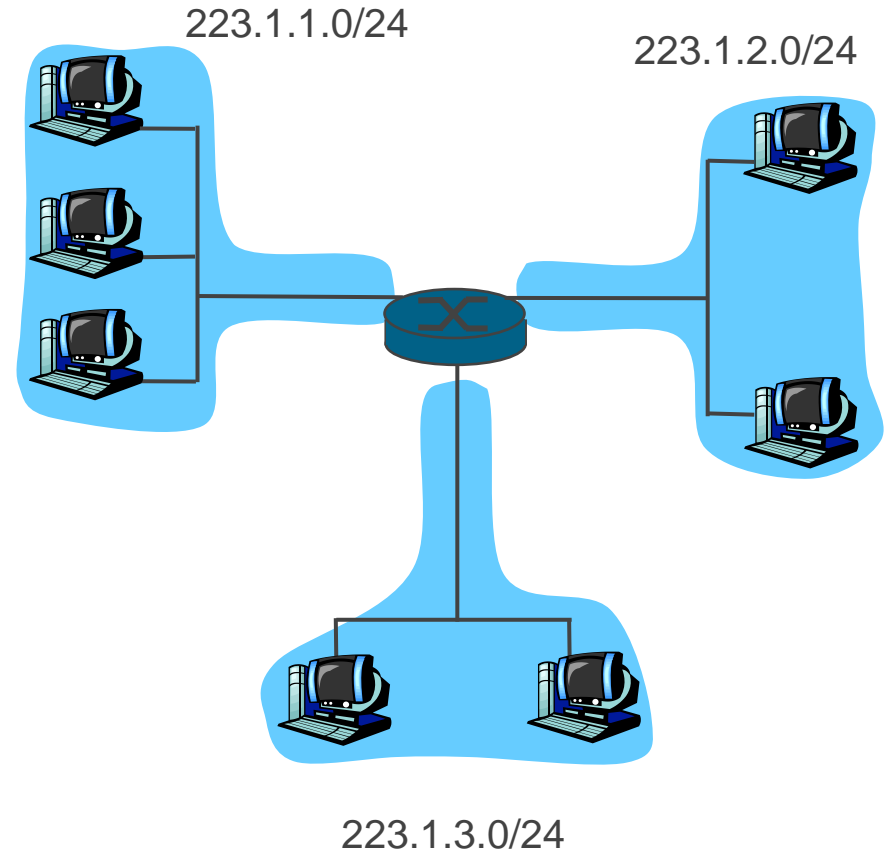
Número de bits a mais a serem utilizados	Número de sub-redes	Número de hosts em cada sub-rede
0	máscara original. rede classe C sem divisão	254
1	0	126
2	2	62
3	6	30
4	14	14
5	30	6
6	62	2
7	126	0
8	endereço de broadcast	-

Como fica a máscara de sub-rede, ao invés de 24 bits, utilizar 27 bits?

Núm. bits	Octeto 01	Octeto 02	Octeto 03	Octeto 04	Nova Máscara
27	11111111	11111111	11111111	11100000	255,255,255,224

## Receita

- para determinar as sub-redes, destaque cada interface de seu hospedeiro ou roteador, criando ilhas de redes isoladas.
- Cada rede isolada é denominada **sub-rede**



Máscara de sub-rede: /24

## CIDR: Classless Inter Domain Routing

*(roteamento interdomínio sem classes)*

- parte de sub-rede do endereço de tamanho arbitrário
- formato do endereço: **a.b.c.d/x**, onde x é # bits na parte de sub-rede do endereço



200.23.16.0/23

# Como listar faixas de IP em cada sub-rede



**Dividir a seguinte rede classe C: 229.45.32.0 / 255.255.255.0.**

São necessárias, pelo menos, 10 sub-redes. Determinar o seguinte:

- a)** Quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes?
- b)** Quantos números IP (hosts) estarão disponíveis em cada sub-rede?
- c)** Qual a nova máscara de sub-rede?
- d)** Listar a faixa de endereços de cada sub-rede.

# Como listar faixas de IP em cada sub-rede



**Dividir a seguinte rede classe C: 229.45.32.0 / 255.255.255.0.**

**a) Quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes?**

Núm. de sub-redes =  $2^n$

Podemos substituir n por valores sucessivos, até atingir ou superar 10.

Ex: para  $n=2$ , a fórmula resulta em 4

$n=3$ , temos 8 sub-redes

$n=4$ , temos 16 sub-redes.

**R: 4 bits.**

# Como listar faixas de IP em cada sub-rede



**b) Quantos números IP (hosts) estarão disponíveis em cada sub-rede?**

Núm. de end. IP dentro de cada sub-rede =  $2^n - 2$

Substituindo n por 4, vou obter um valor de 14.

**R: 14 hosts.**

**c) Qual a nova máscara de sub-rede?**

Como utilizamos 4 bits do último octeto para dividir rede, os 4 primeiros bits da sub-rede foram definidos iguais a 1.

Somar os respectivos valores, ou seja:  $128+64+32+16 = 240$ .

**R: 255.255.255.240**

**229.45.32.0/28**

# Como listar faixas de IP em cada sub-rede



## d) Listar a faixa de endereços de cada sub-rede.

Observar o último bit definido para a máscara. No exemplo é o 4º bit do ultimo. O valor decimal do 4º bit é 16, que indica as faixas de variação.

Tem-se 16 hosts em cada sub-rede (1º e o último não são usados).

<b>Sub-rede 01:</b>	229.45.32.0	->	229.45.32.15
<b>Sub-rede 02:</b>	229.45.32.16	->	229.45.32.31
<b>Sub-rede 03:</b>	229.45.32.32	->	229.45.32.47
<b>Sub-rede 04:</b>	229.45.32.48	->	229.45.32.63
<b>Sub-rede 05:</b>	229.45.32.64	->	229.45.32.79
<b>Sub-rede 06:</b>	229.45.32.80	->	229.45.32.95
<b>Sub-rede 07:</b>	229.45.32.96	->	229.45.32.111
<b>Sub-rede 08:</b>	229.45.32.112	->	229.45.32.127
<b>Sub-rede 09:</b>	229.45.32.128	->	229.45.32.143
<b>Sub-rede 10:</b>	229.45.32.144	->	229.45.32.159
<b>Sub-rede 11:</b>	229.45.32.160	->	229.45.32.175
<b>Sub-rede 12:</b>	229.45.32.176	->	229.45.32.191
<b>Sub-rede 13:</b>	229.45.32.192	->	229.45.32.207
<b>Sub-rede 14:</b>	229.45.32.208	->	229.45.32.223
<b>Sub-rede 15:</b>	229.45.32.224	->	229.45.32.239
<b>Sub-rede 16:</b>	229.45.32.240	->	229.45.32.255

# Endereços IP: como obter um?

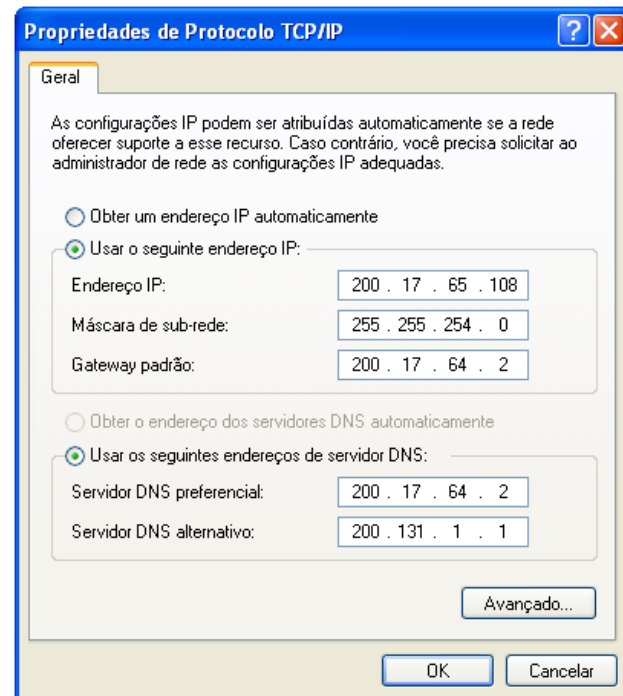
**P:** Como um *hospedeiro* obtém endereço IP?

fornecido pelo administrador do sistema em um arquivo

- Windows: painel de controle → rede → configuração → tcp/ip → propriedades
- UNIX: /etc/rc.config

**DHCP** (Dynamic Host Configuration Protocol):

- recebe endereço dinamicamente servidor
  - “plug-and-play”

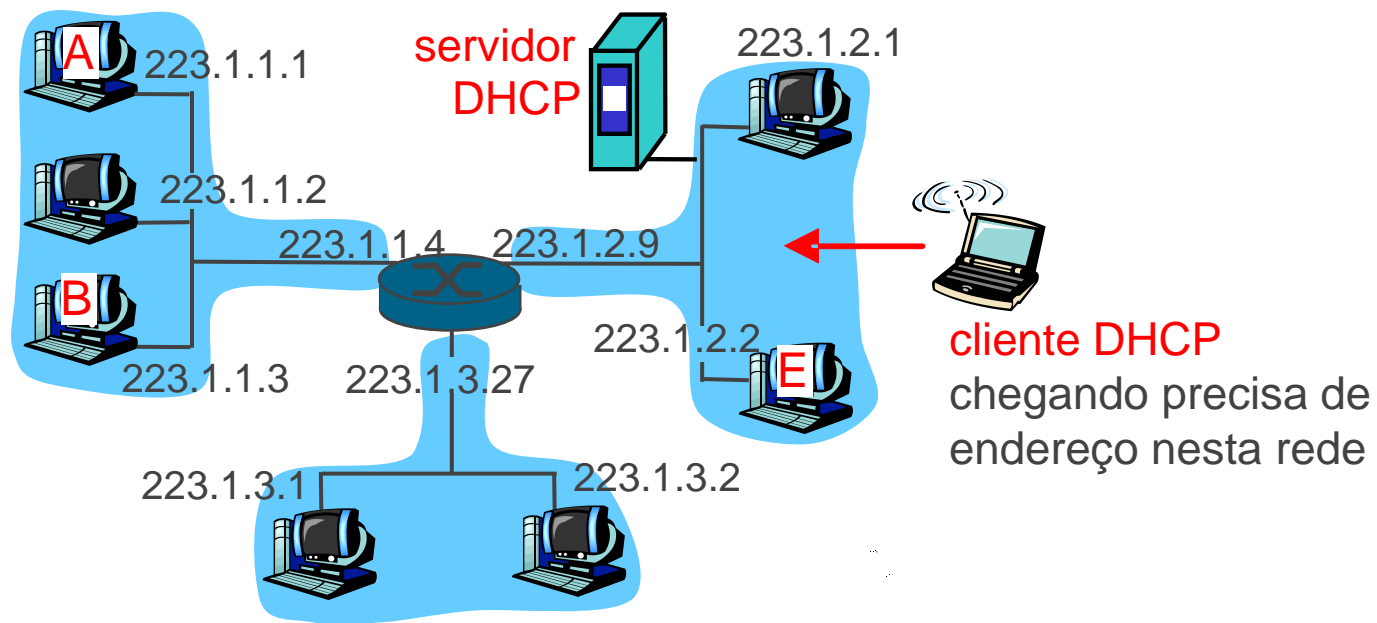




**Objetivo:** permitir que o host obtenha *dinamicamente* seu endereço IP do servidor de rede quando se conectar à rede.

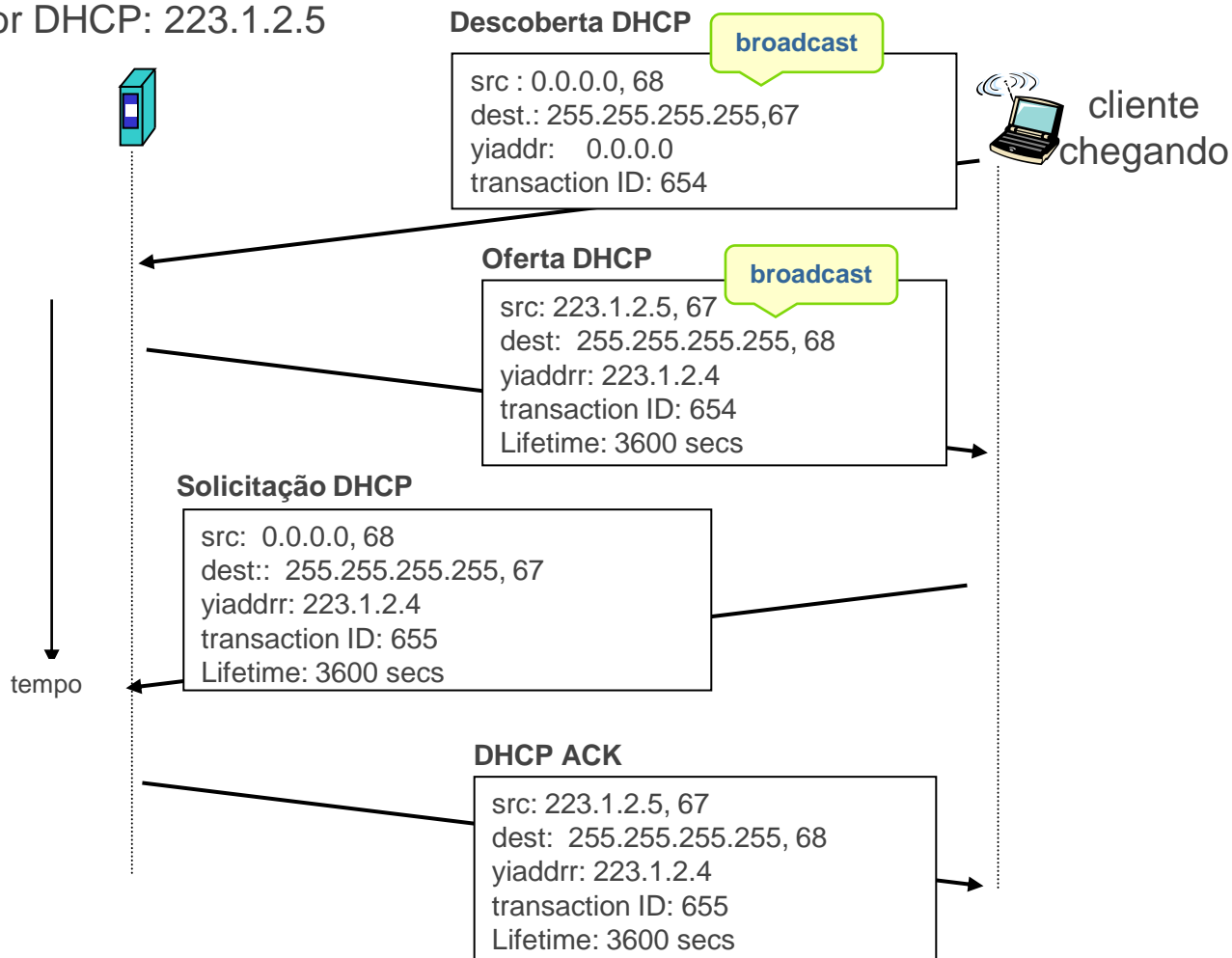
- pode renovar seu prazo no endereço utilizado;
- permite reutilização de endereços (só mantém endereço enquanto conectado e “ligado”);
- aceita usuários móveis que queiram se juntar à rede (mais adiante).
- No caso de um ISP, economia de endereços IPs

# DHCP – cenário cliente/servidor



# DHCP – cenário cliente/servidor

servidor DHCP: 223.1.2.5



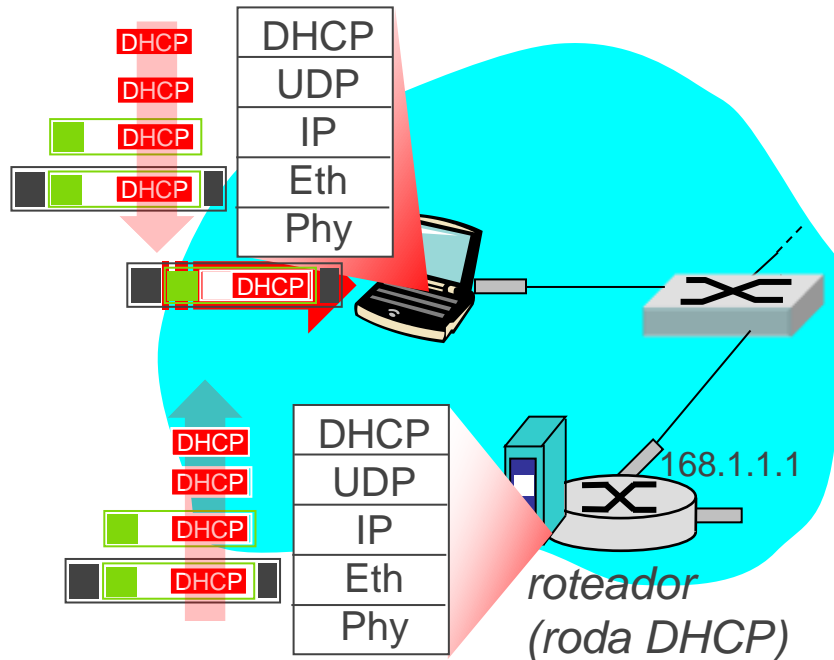
# DHCP: mais do que endereço IP



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

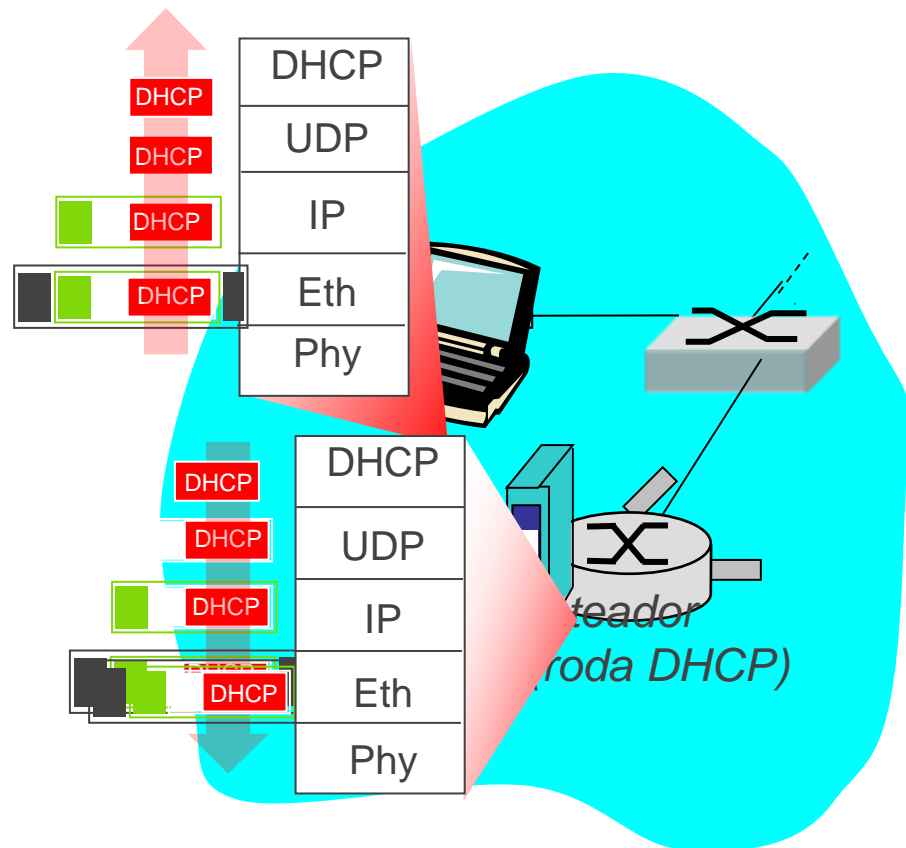
- endereço do roteador/gateway do 1º salto para o cliente
- nome e endereço IP do servidor DNS
- máscara de rede (indicando parte de rede vs host)

# DHCP: exemplo



- conexão de laptop precisa do seu endereço IP, endereço do roteador do primeiro salto, endereço do servidor DNS: use DHCP
- solicitação DHCP encapsulada no UDP, encapsulada no IP, encapsulado no Ethernet 802.3
- broadcast de quadro Ethernet (dest: FFFFFFFFFFFFFFFF) na LAN, recebido no roteador rodando DHCP
- Ethernet demultiplexado para IP demultiplexado, UDP demultiplexado para DHCP

# DHCP: exemplo



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

# Endereçamento IP: gestão

- **P:** Como um ISP recebe bloco de endereços?
- **RIR** (Regional Internet Registries): responsáveis pela distribuição, gerenciamento e registro dos endereços IPv4 e IPv6.
  - Ligadas à [IANA](http://iana.org) (*Internet Assigned Numbers Authority*)

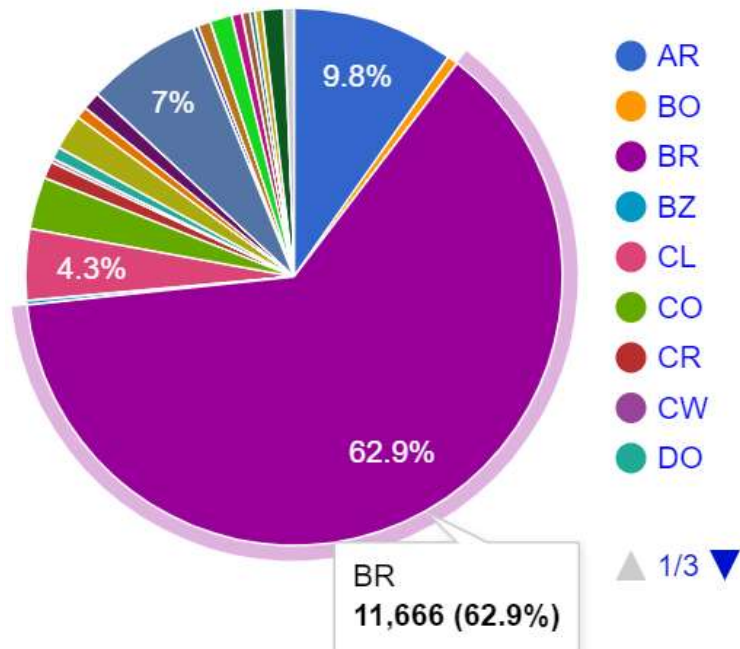


# Endereçamento IP: gestão

## LACNIC: Latin America and Caribbean Network Information Centre

- É a organização responsável pela alocação e administração dos Endereçamentos IP para a América Latina e Caribe.
- É um dos 5 Registros Regionais da Internet no mundo.

Distribuição de blocos IPv4 por país



Prof. Marlon Paolo



# Endereçamento IP: a última palavra...

**ICANN:** Internet Corporation for Assigned Names and Numbers

- **Responsável pela governança global da Internet no que se referia à distribuição de endereços IP.**
  - aloca endereços
  - administra o DNS
    - Coordena, através do DNS Root Server System Committee, as organizações que operam os atuais 13 servidores-raiz do DNS.
  - atribui nomes de domínio e resolve disputas

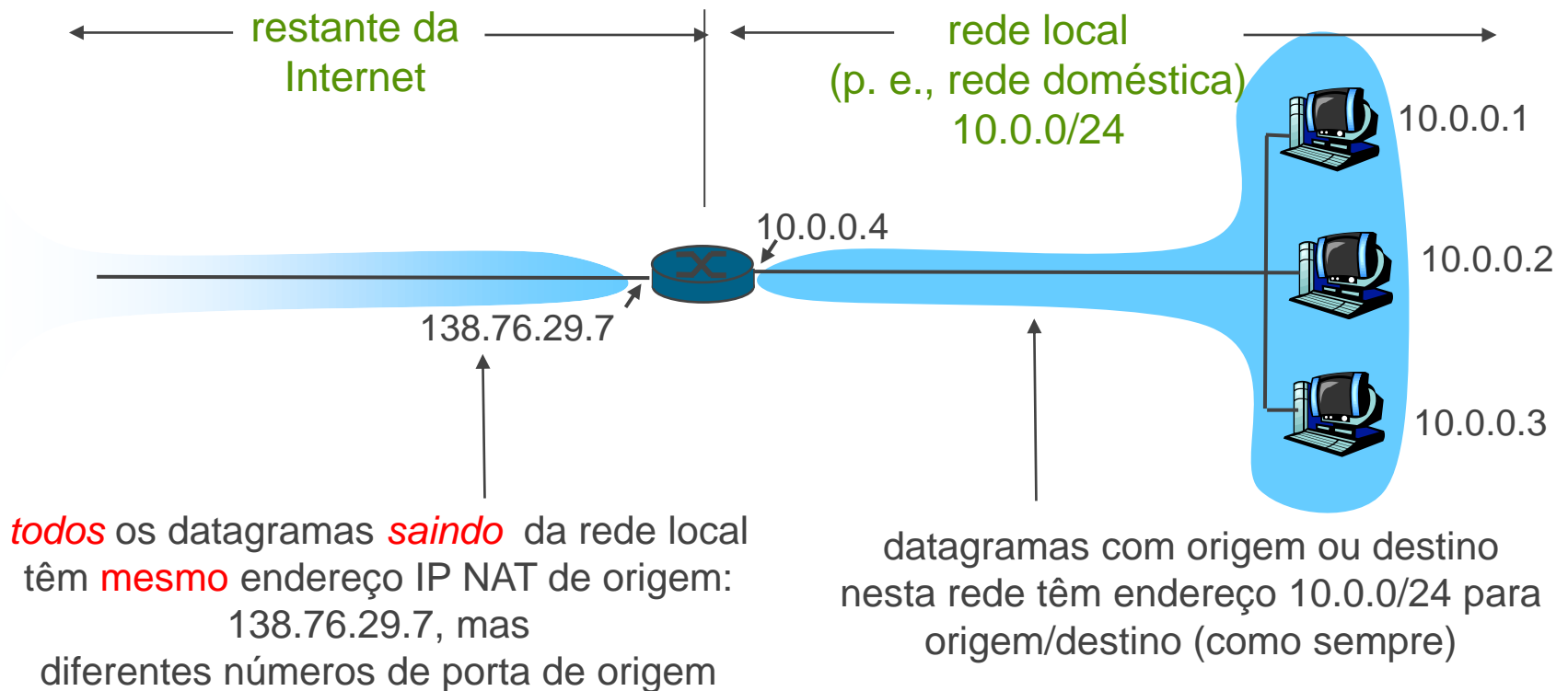


- **motivação:** alternativa viável para o problema de falta de endereços IP v4 na Internet.
  - rede local usa apenas 1 endereço IP válido para navegação para todos os dispositivos;
  - pode mudar os endereços dos dispositivos na rede local sem notificar o mundo exterior;
  - pode mudar de ISP sem alterar os endereços dos dispositivos na rede local;
  - dispositivos dentro da rede local não precisam ser explicitamente endereçáveis ou visíveis pelo mundo exterior (uma questão de segurança).

- **Endereços privados não podem ser utilizados diretamente na Internet.**
  - Roteadores da Internet estão configurados para descartar pacotes com origem ou destino dentro das faixas de endereços IP privados.
    - 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16
- **Perguntas:**
  - 1. Como é possível a comunicação de mais de um cliente, ao mesmo tempo, com a Internet, já que todo o tráfego da rede sairá com o mesmo IP?
  - 2. Quando a resposta retorna, como o NAT sabe para qual cliente da LAN ela se destina, se houver mais usuários acessando a Internet?

# NAT: Network Address Translation

**Tradução de endereços:** *traduzir de um endereço IP interno, não válido na Internet para um endereço IP válido na Internet.*



## Implementação → roteador NAT deve:

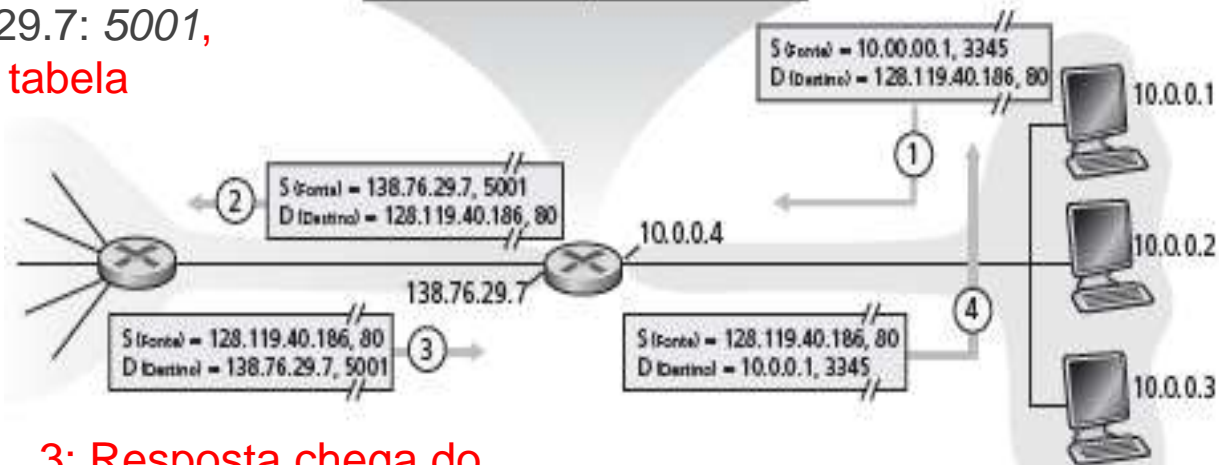
- **enviando datagramas:** *substituir* (IP de origem, # porta) de cada datagrama saindo por um válido (IP da NAT, nova # porta)
- O NAT mantém uma **tabela interna** onde fica registrado que, *comunicação através da porta “tal” está relacionada com o cliente “tal”*.
- Ex: tabela do NAT, em um determinado momento, poderia ter o seguinte:
  - 144.72.3.21:6555      10.10.0.10
  - 144.72.3.21:6556      10.10.0.11
  - 144.72.3.21:6557      10.10.0.12
  - 144.72.3.21:6558      10.10.0.13
  - 144.72.3.21:6559      10.10.0.14
- **recebendo datagramas:** *substituir* (endereço IP da NAT, nova # porta) nos campos de destino de cada datagrama chegando por (endereço IP origem, # porta) correspondente, armazenado na tabela NAT.

# NAT: Network Address Translation

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

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

1: hospedeiro 10.0.0.1 envia datagrama para 128.119.40.186: 80



3: Resposta chega do endereço destino: 138.76.29.7: 5001

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

- **campo de número de porta de 16 bits:**
  - 60.000 conexões simultâneas com um único endereço no lado da LAN!
  - os endereços da LAN são “traduzidos” para o mesmo endereço externo, porém com um número diferente de porta para cada cliente da rede interna.
- **Uma vez habilitado o NAT, este passa a ser um servidor DHCP para a rede interna, fornecendo as configurações do TCP/IP para os clientes da LAN.**
  - Para o esquema de endereçamento da rede interna, deve-se utilizar uma faixa de endereços privados.

- **NAT é controverso:** puristas têm grandes restrições à NAT
  - Uma das premissas da RFC 791 é que cada host conectado à Internet deve ter um endereço único.
  - Roteadores só devem processar até a camada 3
  - Viola argumento de fim a fim
    - a possibilidade de NAT deve ser levada em conta pelos projetistas da aplicação, p. e., aplicações P2P;
  - A falta de endereços é resolvida pelo IPv6;
  - Aumento do processamento no dispositivo tradutor;
  - Impossibilidade de se rastrear o caminho do pacote;
  - Impossibilita a utilização de algumas técnicas de segurança como IPSec.



- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - **ICMP**
  - IPv6
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

# ICMP: Internet Control Message Protocol

- **usado por hospedeiros & roteadores para comunicar informações em nível de rede**

- relato de erro: hospedeiro, rede, porta, protocolo inalcançável
- eco de solicitação/ resposta (usado por ping)

- **camada de rede “acima” do IP:**

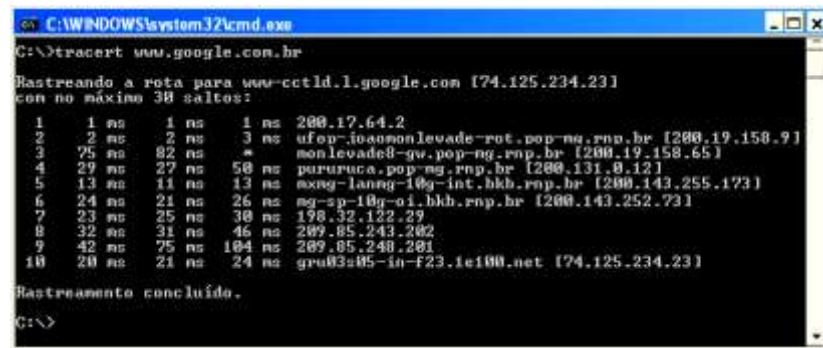
- msgs ICMP transportadas em datagramas IP

- **mensagem ICMP: tipo, código mais primeiros 8 bytes do datagrama IP causando erro**

Tipo	Cód.	Descrição
0	0	resposta de eco (ping)
3	0	rede de destino inalcançável
3	1	hosp. de destino inalcançável
3	2	protocolo de destino inalcançável
3	3	porta de destino inalcançável
3	6	rede de destino desconhecida
3	7	hosp. de destino desconhecido
4	0	redução da fonte (controle de congestionam. – não usado)
8	0	solicitação de eco (ping)
9	0	anúncio de rota
10	0	descoberta do roteador
11	0	TTL expirado
12	0	cabeçalho IP inválido

# Traceroute e ICMP

- origem envia série de segmentos UDP ao destino
  - primeiro tem TTL = 1
  - segundo tem TTL = 2 etc.
  - número de porta improvável
- datagrama n chega ao n roteador:
  - roteador descarta datagrama
  - e envia à origem uma msg ICMP (tipo 11, código 0)
  - mensagem inclui nome do roteador & endereço IP
- quando a mensagem ICMP chega, origem calcula RTT
- traceroute faz isso 3 vezes



```
C:\WINDOWS\system32\cmd.exe
C:\>tracert www.google.com.br

Rastreando a rota para www-ccldl1.google.com [74.125.234.23]
con no máximo 30 saltos:

 1  1 ms  1 ms  1 ms  200.17.64.2
 2  2 ms  2 ms  3 ms  ufop-joaomonlevade-rot.pop-ng.rnp.br [200.19.158.9]
 3  75 ms 82 ms *      monlevade8-gw.pop-ng.rnp.br [200.19.158.65]
 4  29 ms 27 ms 50 ms  pururaca.pop-ng.rnp.br [200.131.0.12]
 5  13 ms 11 ms 13 ms  mong-lanng-10g-int.hkb.rnp.br [200.143.255.173]
 6  24 ms 21 ms 26 ms  ng-sp-10g-oi.hkb.rnp.br [200.143.252.73]
 7  23 ms 25 ms 30 ms  198.32.122.29
 8  32 ms 31 ms 46 ms  209.85.243.202
 9  42 ms 75 ms 104 ms 209.85.240.201
10  20 ms 21 ms 24 ms  gru03s05-in-f23.1e100.net [74.125.234.23]

Rastreamento concluído.
C:\>
```

## Critério de término

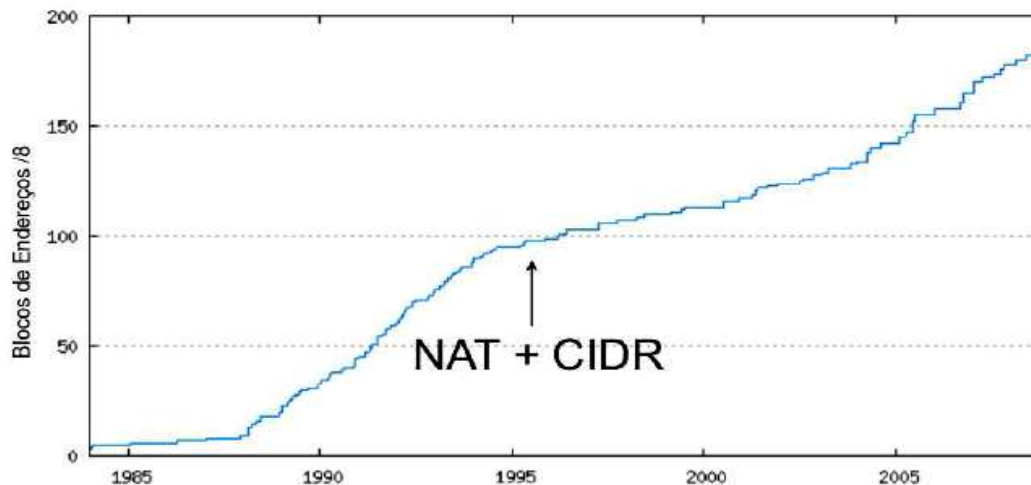
- segmento UDP por fim chega no host destino (com um n° de porta improvável)
- destino retorna pacote ICMP “host inalcançável” (tipo 3, código 3)
- quando origem recebe esse ICMP, termina.

- 4. 1 Introdução
- 4.2 Redes de circuitos virtuais e de datagramas
- **4.3 IP: Internet Protocol**
  - formato do datagrama
  - endereçamento IPv4
  - ICMP
  - **IPv6**
- **4.4 Algoritmos de roteamento**
  - estado de enlace
  - vetor de distâncias
  - roteamento hierárquico

# Desenvolvimento do IPv6

- Medidas como NAT e CIDR geraram mais tempo para desenvolver uma nova versão do IP.
- 1992 - IETF cria o grupo IPng (IP Next Generation)
  - **Principais questões:** Escalabilidade, Segurança; Mobilidade, Suporte a QoS, Políticas de roteamento, Transição.

## Soluções paliativas: Queda de apenas 14%



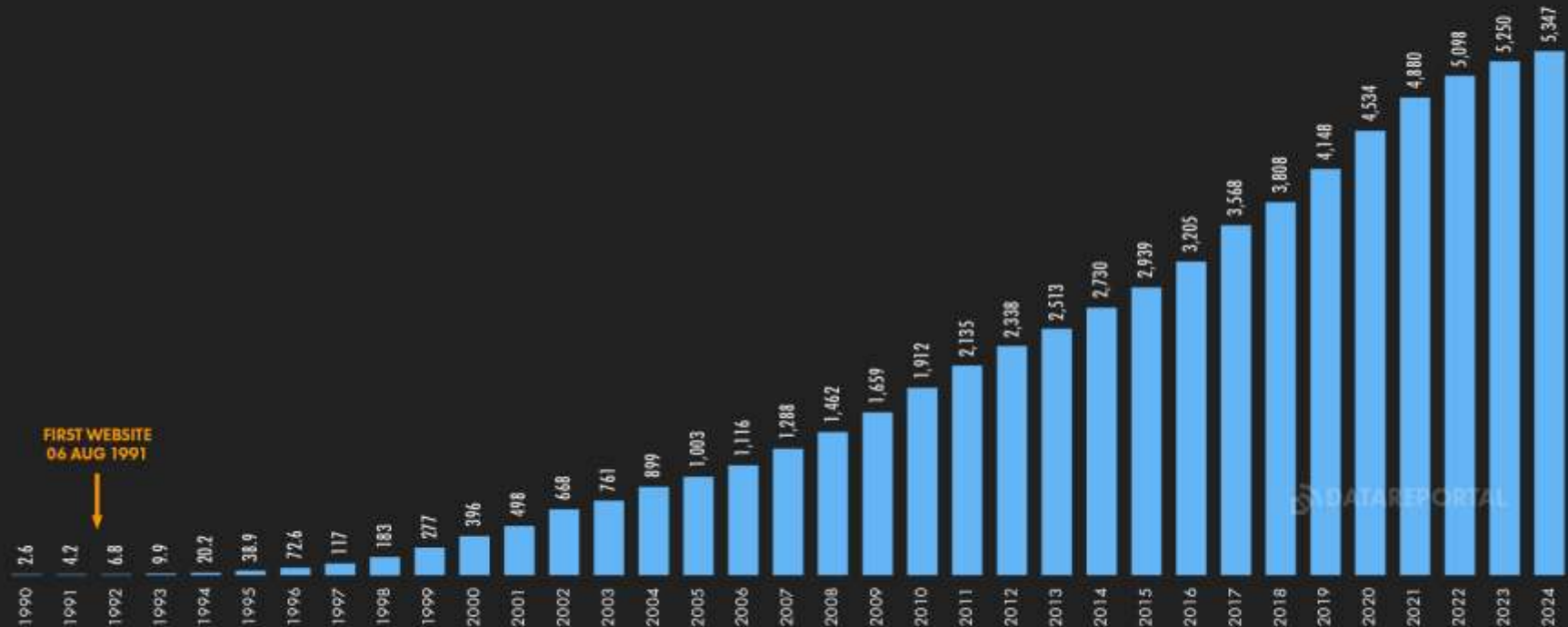
- 1998 – IPv6 Definido pela RFC 2460

# Por que utilizar IPv6 hoje?

JAN  
2024

## INTERNET USE TIMELINE

NUMBER OF INDIVIDUALS USING THE INTERNET OVER TIME (IN MILLIONS)



FIRST WEBSITE  
06 AUG 1991

**SOURCES:** KPIVOS ANALYSIS, IFA, GSMA INTELLIGENCE, EUROSTAT, GOOGLE'S ADVERTISING RESOURCES, CNNIC, KANTAR & IAMA, GOVERNMENT RESOURCES, UNITED NATIONS. **COMPARABILITY:** SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCES DO NOT PUBLISH REGULAR UPDATES, SO FIGURES FOR RECENT PERIODS MAY UNDER-REPRESENT ACTUAL USE. SEE [NOTES ON DATA](#).

# Por que utilizar IPv6 hoje?

- **motivação inicial:** espaço de endereço de 32 bit logo estará completamente alocado

Registros Regionais entraram em fases de esgotamento como mostrado abaixo:

RIR	Estado recursos IPv4
APNIC	Começou a usar o último /8 em abril de 2011.
RIPE	Começou a usar o último /8 em 14 de setembro de 2012.
LACNIC	Começo da phase 3: 15/Fev/2017
ARIN	Encontra-se na fase 4 de esgotamento (último /8 a partir de 24/04/2014). A partir de 01/07/2015 políticas de lista de espera para os pedidos não satisfeitos.
AFRINIC	Único registro que vai ter endereços durante vários anos.

# Por que utilizar IPv6 hoje?



- A Internet continua crescendo...

## Mundo

- 5.300.000.000 de usuários com acesso à Internet;
  - *A cada dia 500 mil pessoas entram pela primeira vez na Internet !!!!*
- Crescimento de 444,8% nos últimos 10 anos.
  - *Em 2023 são **30 bilhões** de dispositivos (smartphones, notebooks, PC, smart TVs, consoles, tablets e modems).... IoT !!!!*

## Brasil

- 84 % de domicílios com acesso à Internet;

Dados: Nov/2023



# Por que utilizar IPv6 hoje?



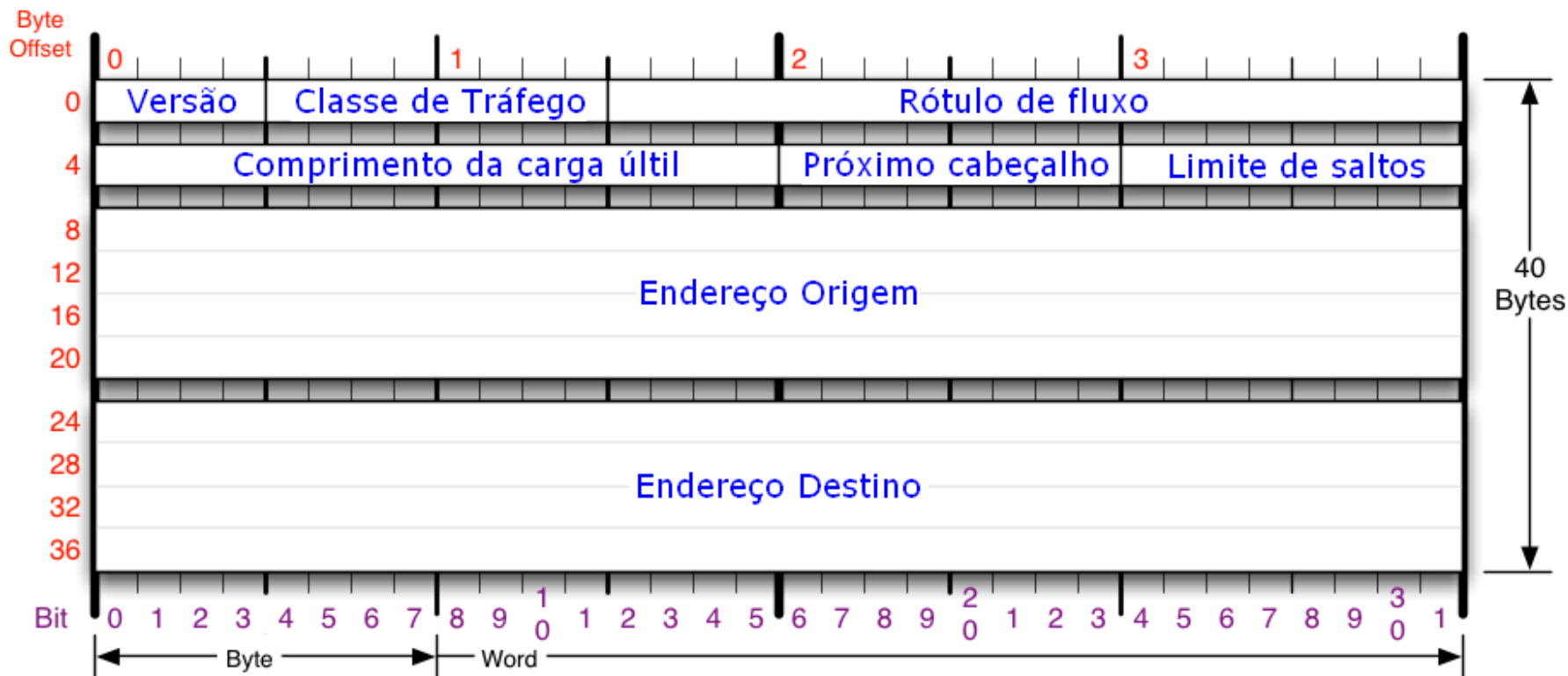
- **motivação adicional:**

- formato de cabeçalho ajuda a agilizar processamento e repasse
- mudanças para facilitar QoS
  - Ex: transmissão de áudio e vídeo poderia ser trados como um fluxo, e transferência de arquivos e e-mail não
  - Definições de prioridades → Ex: pacotes ICMP

## formato de datagrama IPv6:

- cabeçalho de 40 bytes de tamanho fixo
- fragmentação não permitida
  - A rede possui mecanismos para descobrir a MTU do caminho

# Cabeçalho IPv6



*Classe de tráfego:* identificar prioridade entre datagramas no fluxo

*rótulo de fluxo:* identificar datagramas no mesmo "fluxo." (pouco definido)

*próximo cabeçalho:* identifica protocolo da camada superior para dados.

# Cabeçalho IPv6 - mudanças do IPv4

IPv4

Version	Hlen	TOS	Length	
Ident		Flags	Offset	
TTL	Protocol		Checksum	
Source Address				
Destination Address				
Options (variable)			Pad (variable)	
Data				

☐ Cabeçalhos novos  
☐ Cab. Removidos

IPv6

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

- 6 campos do cabeçalho IPv4 foram removidos.
- 4 campos tiveram nomes alterados e seus posicionamentos modificados.
- O campo Identificador de Fluxo foi acrescentado.

# Outras mudanças do IPv4



- **soma de verificação:** removida inteiramente para reduzir tempo de processamento em cada salto
- **opções:** permitidas, mas fora do cabeçalho, indicadas pelo campo de “Próximo Cabeçalho”
- **ICMPv6:** nova versão do ICMP
  - tipos de mensagem adicionais, p. e. “Pacote Muito Grande”
  - funções de gerenciamento de grupo multicast

- Um endereço IPv4 é formado por 32 bits.

$$\bullet 2^{32} = 4.294.967.296$$

- Um endereço IPv6 é formado por 128 bits.

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

~ 56 octilhões ( $5,6 \times 10^{28}$ ) de endereços IP por ser humano.

~ 79 octilhões ( $7,9 \times 10^{28}$ ) de vezes a quantidade de endereços IPv4.

~ 1 IP para cada grão de areia

# Endereçamento IPv6

- Representação dos endereços, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais.

- **2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1**

- Na representação de um endereço IPv6 é permitido:

- Utilizar caracteres maiúsculos ou minúsculos;
- Omitir os zeros à esquerda; e
- Representar os zeros contínuos por “::”.

- Exemplo:

- **2001:0DB8:0000:0000:130F:0000:0000:140B**

- **2001:db8:0:0:130f::140b**

- **Formato inválido: 2001:DB8::130F::140B (gera ambiguidade)**

- Representação dos Prefixos
  - Como o CIDR (IPv4)
    - “endereço-IPv6/tamanho do prefixo”
  - Exemplo:
    - Prefixo 2001:db8:3003:2::/64
    - Prefixo global 2001:db8::/32
- Representação dos endereços IPv6 em URLs
  - Endereços representados entre colchetes (não gera ambiguidade caso necessário indicar o número de porta junto com a URL)
    - [http://\[2001:12ff:0:4::22\]/index.html](http://[2001:12ff:0:4::22]/index.html)
    - [http://\[2001:12ff:0:4::22\]:8080](http://[2001:12ff:0:4::22]:8080)

# Transição de IPv4 para IPv6

- **Como a Internet pública, baseada em IPv4 fará a transição para o IPv6?**
  - como a rede operará com roteadores IPv4 e IPv6 misturados?
- **Dia de conversão?**
  - Uma data e horário determinado em que todas as máquinas **IPv4** da Internet seriam desligadas?
- **nem todos os roteadores podem ser atualizados simultaneamente**
  - sem “dia de conversão”
- ***Implantação de túnel:***
  - IPv6 transportado como carga útil no datagrama IPv4 entre roteadores IPv4
  - Quando pacote chegar a um router IPv6, extrai o datagrama IPv6 e o roteia normalmente

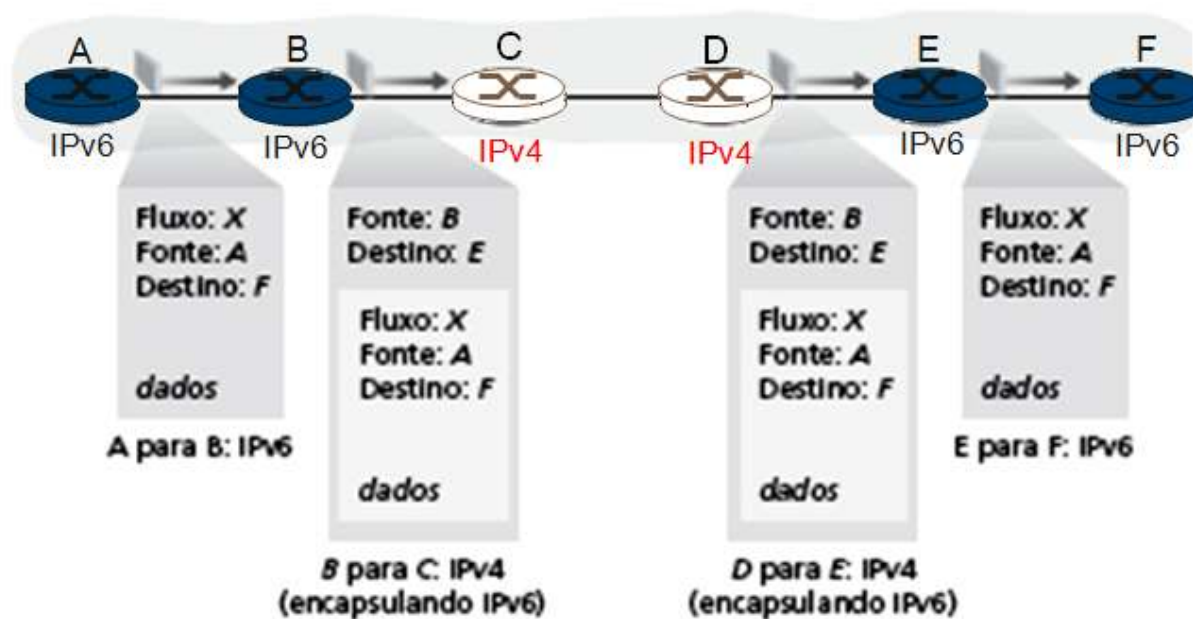


# Implantação de túnel

Visão lógica:



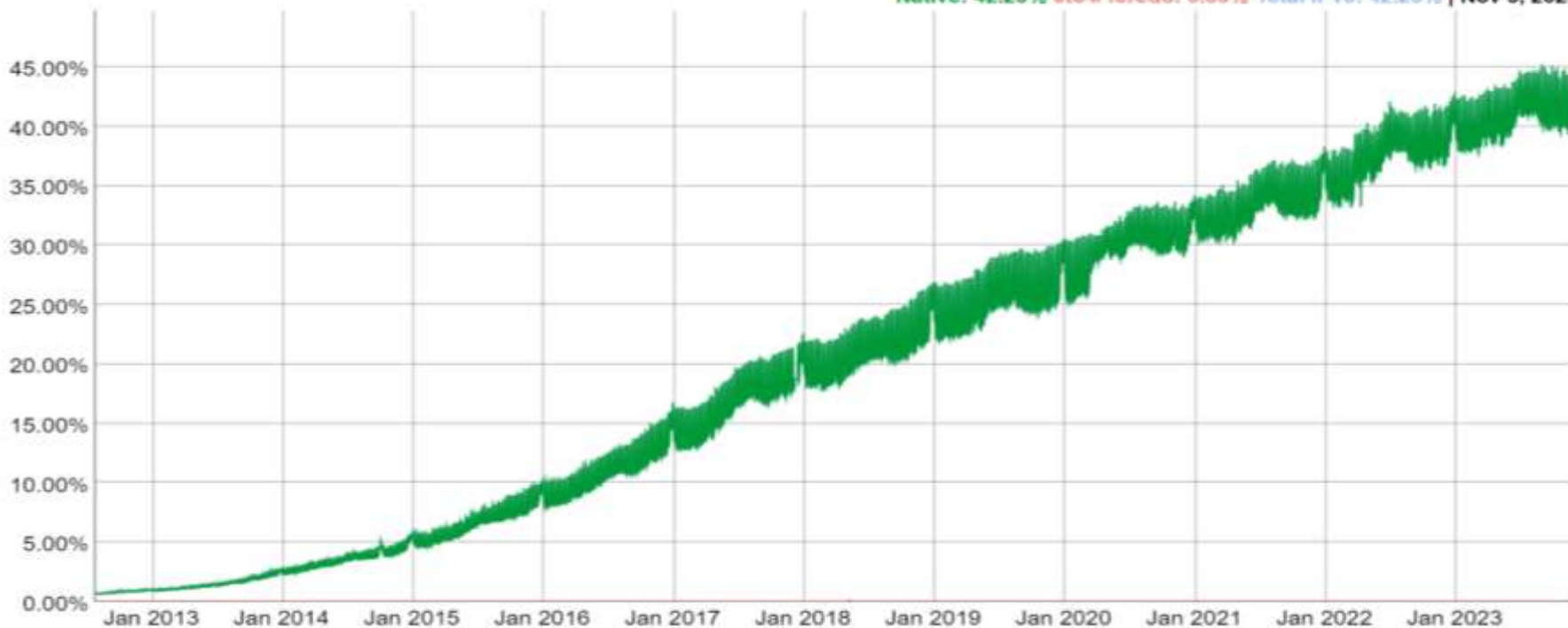
Visão física:



# Como está a implantação do IPv6?

- 32 % dos ASs trabalham sobre IPv6
- Os 13 root DNS servers são acessíveis via IPv6
- 45% de clientes do Google possuem IPv6 ativado

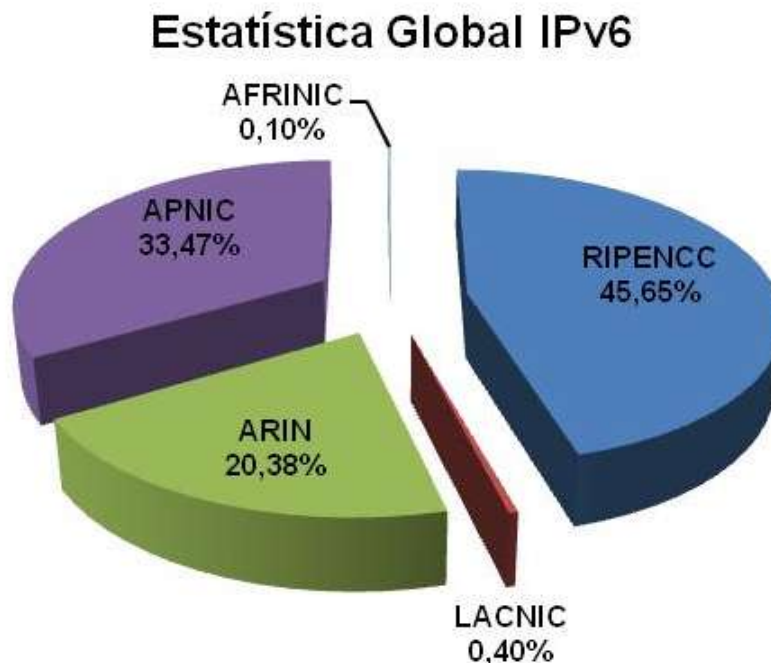
Native: 42.23% 6to4/Teredo: 0.00% Total IPv6: 42.23% | Nov 3, 2023



- Dos ~73.000 blocos /32 já alocados pelos RIR, apenas 5% são efetivamente utilizados.

# Como está a implantação do IPv6 no Brasil?

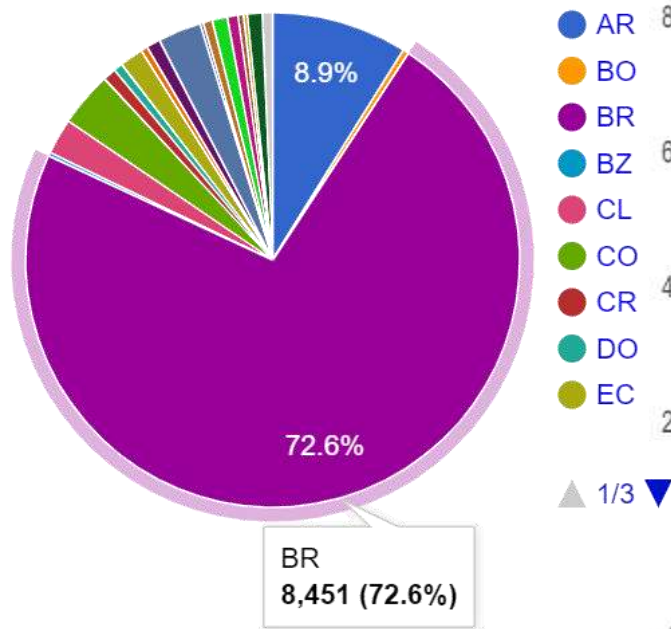
- Os blocos atribuídos para o LACNIC correspondem a apenas 0,4% dos já atribuídos mundialmente;
- Destes 0,4%, 13,5% estão alocados para o Brasil!
- Porém, dos blocos alocados para o Brasil, apenas 30% estão sendo efetivamente utilizados.



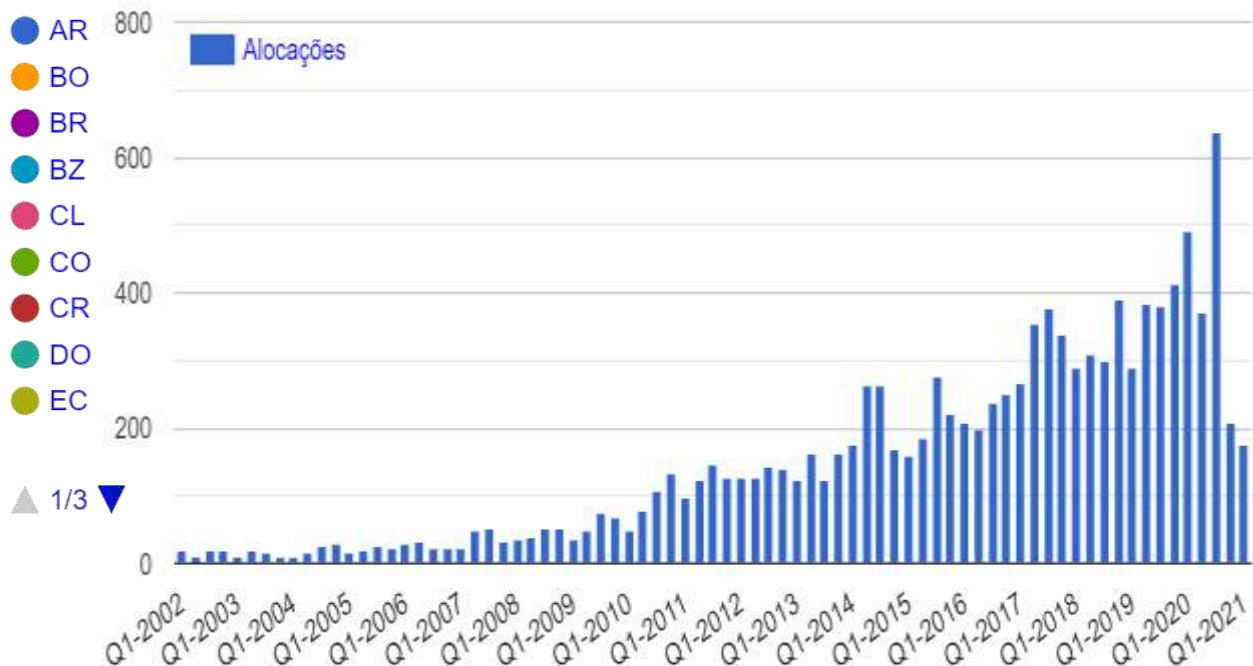
# IPv6: estatística

- Distribuição do IPv6: crescimento constante

Distribuição de blocos IPv6 por país



Total de blocos IPv6 alocados (16 e 32 bits)



# Implantação do IPv6: dificuldades

- A completa implantação do IPv6 está levando um bom tempo .....
- Motivo: enorme dificuldade para mudar protocolos da camada de rede.
  - **Analogia:** *é como substituir as fundações de uma casa*
  - *Difícil fazer sem demolir a casa inteira ou, no mínimo, retirar os moradores temporariamente da residência.*
  - **Necessário capacitação de profissionais para administrar as redes IPv6.**
  - **Necessário atualização dos dispositivos da rede (software / hardware)**
- Em contrapartida, a Internet vem mudando muito, com a disponibilização de novos protocolos da camada de aplicação...
  - **Analogia:** *é fácil mudar as janelas ou a cor da tinta de uma casa...*