Camada de Rede

Sumário

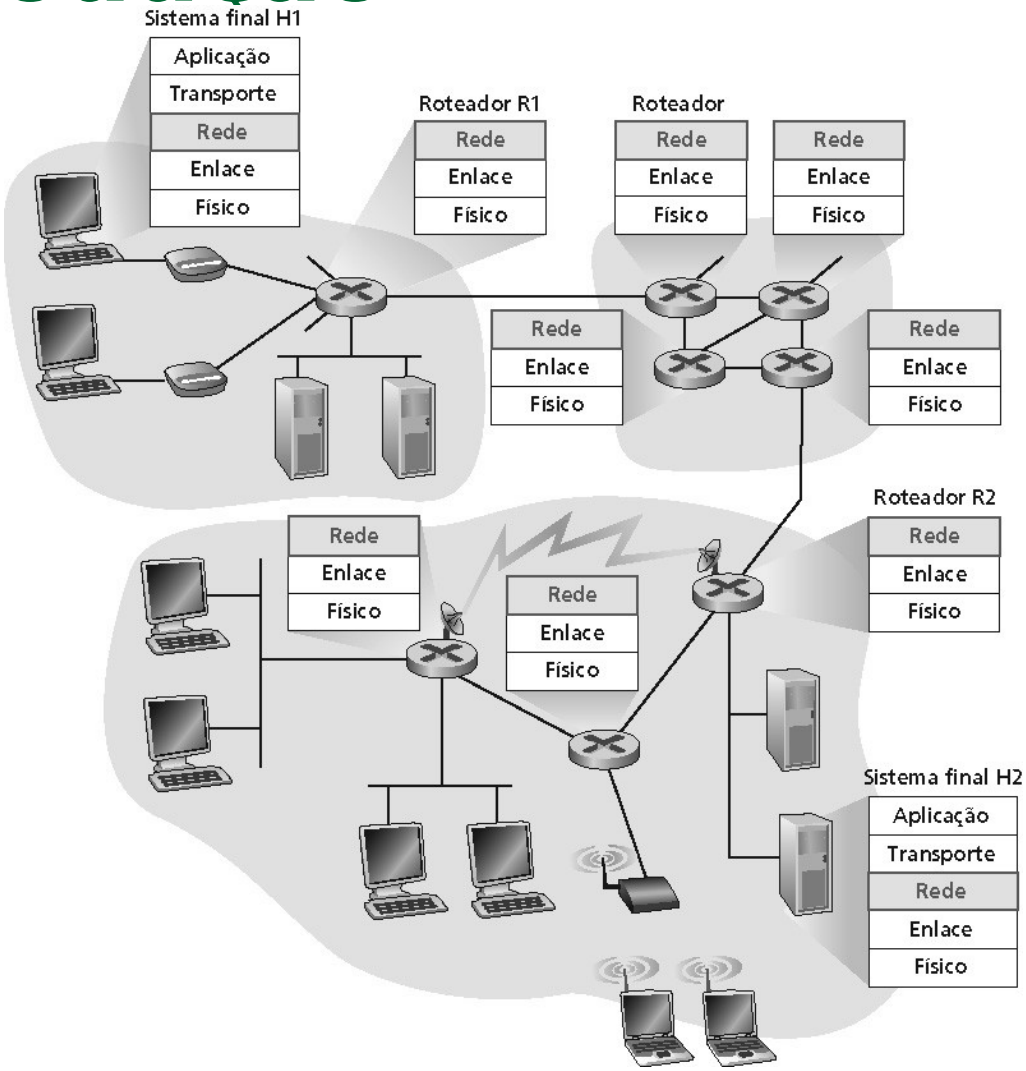
- Introdução;
- Internet Protocol – IP;
- Fragmentação do Datagrama IP;
- Endereço IP;
- Sub-Redes;
- CIDR – Classes Interdomain Routing
- NAT – Network Address Translation

Sumário

- ICMP – Internet Control Message Protocol;
- IPv6;

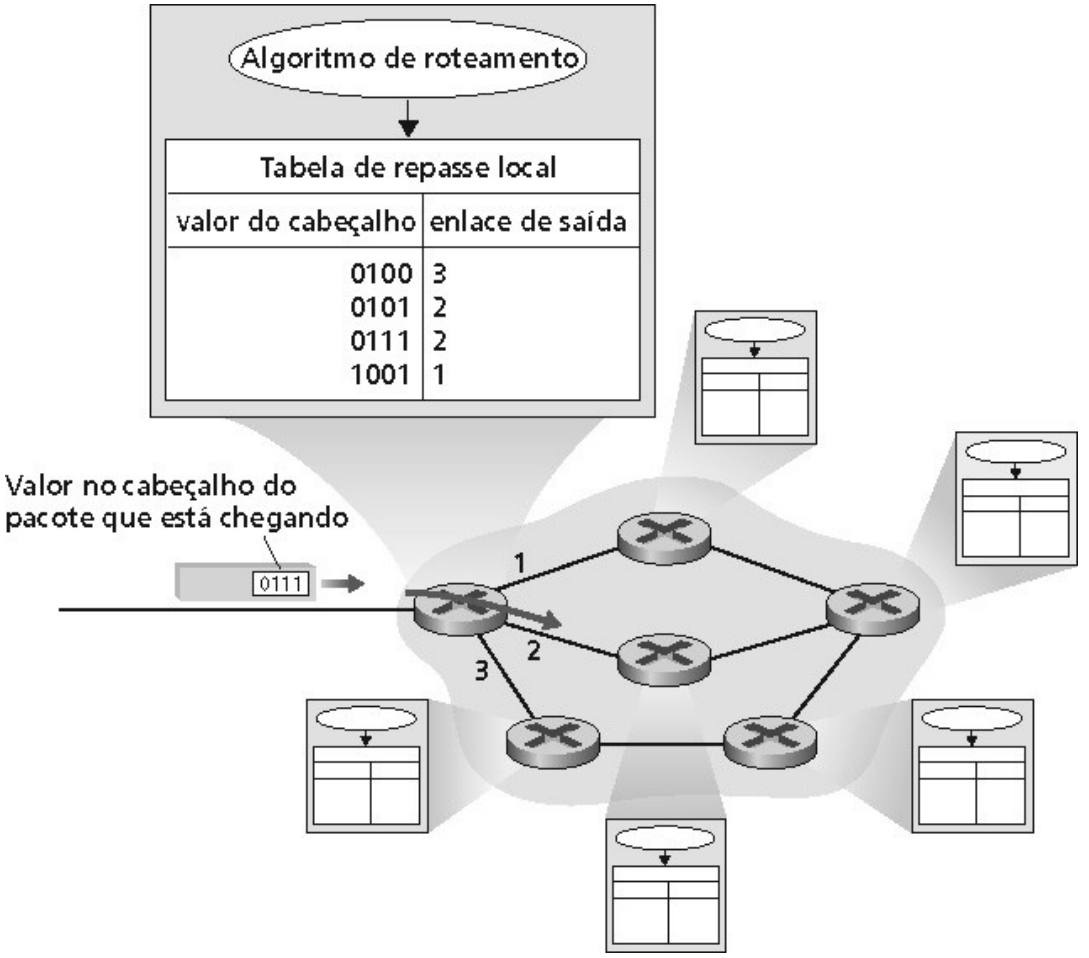
Introdução

- A camada de Rede está relacionada à transferência de pacotes da origem para o destino.
- Chegar ao destino pode exigir vários hops (saltos) em roteadores intermediários ao longo do percurso:



Introdução

- Para atingir seus objetivos, a camada de rede deve conhecer a topologia da sub-rede de comunicações (roteadores) e escolher os caminhos mais apropriados;
  - Evitar ociosidade em algumas rotas e sobrecarga em outra



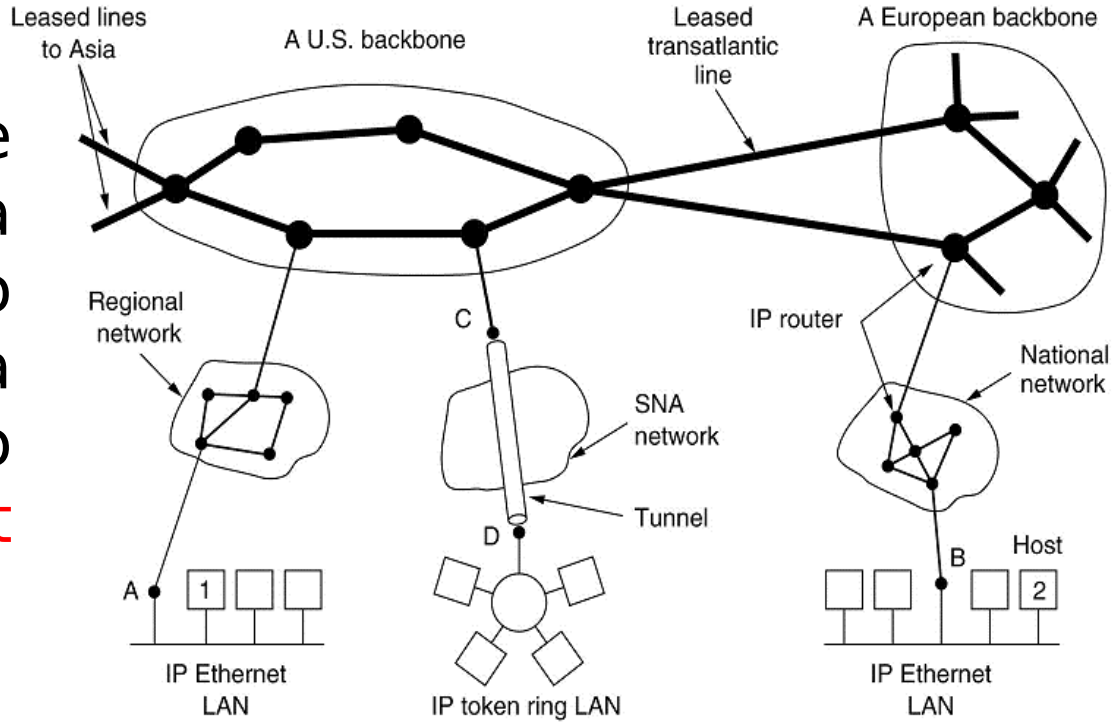
Introdução

- Dessa forma, veja os principais pontos que serão abordados sobre a camada de rede:
  - Algoritmos de Roteamento;
  - Algoritmos de Controle e Congestionamento;
  - Qualidade de Serviço;
  - Interligação de Redes;
  - Protocolo da Internet (IP);

Internet Protocol - IP

- Como bem sabemos, a Internet é um conjunto de muitas redes interconectadas:

- O elemento que mantém a Internet unida é o protocolo da camada de rede o IP (Internet Protocol);



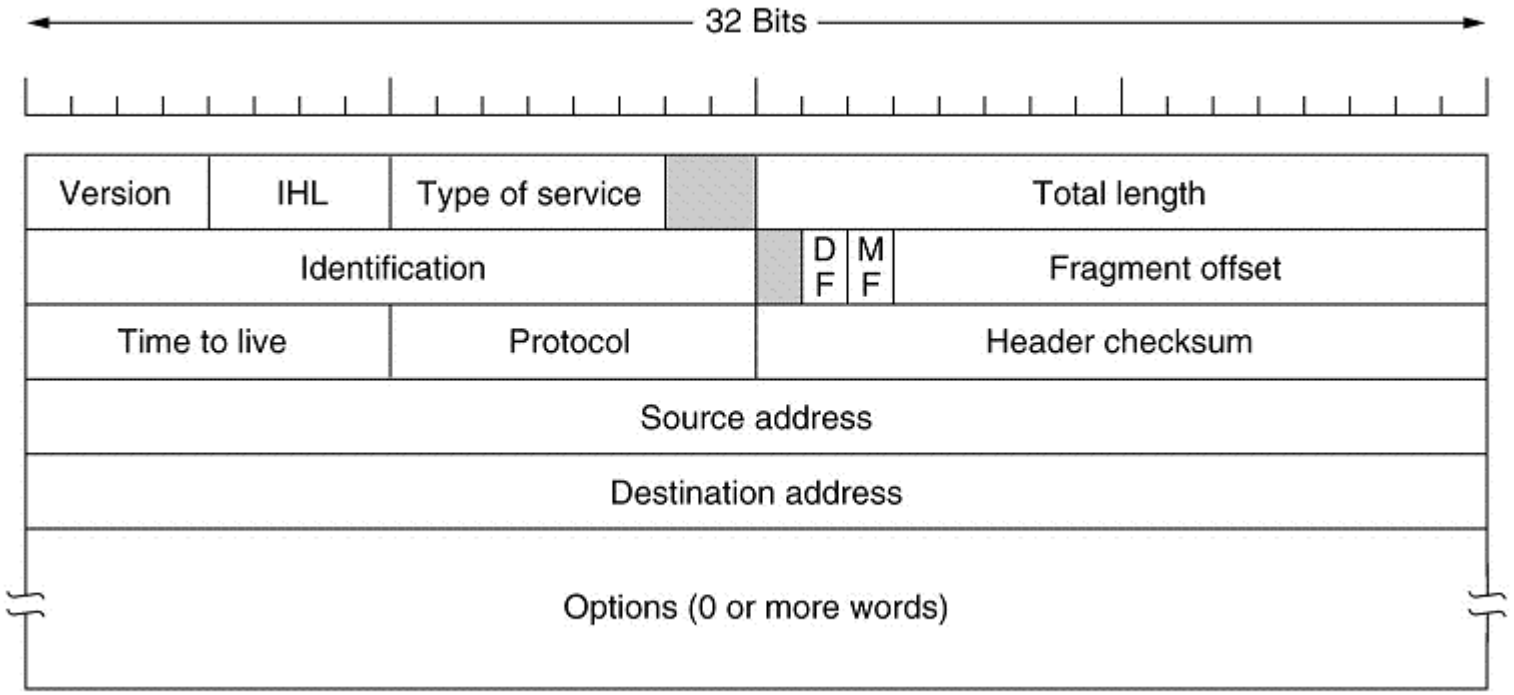
Internet Protocol - IP

- A tarefa do IP é fornecer a melhor forma possível (sem garantias) de transportar datagramas (pacotes da camada de Rede) da origem para o destino, independentemente de essas máquinas estarem na mesma rede ou de haver outra redes entre elas;

- Há duas versões de protocolo IP em uso hoje:
  - IPv4 [RFC 791]
  - Ipv6 [RFC 2373; RFC 2460]

Internet Protocol - IP

- Vejamos como é formado um datagrama Ipv4:



Internet Protocol - IP

- Considerações:
  - Version: indica a cersão do protocolo (4 para Ipv4);
  - IHL: tamanho do cabeçalho em palavras de 32 bits;
  - Type of Service: Serviço requerido;
  - Total lenght: tamanho total do pacote (cabeçalho + dados);
  - Identification: Identifica cada pacote enviado por um nó;
  - DF (Don't Fragment): desautoriza a fragmentação do pacote porque o destino não será capaz de recompô-lo
  - MF (More Fragment): indica que há outros fragmentos (bit 1 para o último fragmento);
  - Fragment Offset: indica a localização deste fragmento no pacote completo

Internet Protocol - IP

- Considerações:
  - Time to Live: Tempo de vida, decrementado a cada nó intermediário, indicando o número máximo de encaminhamentos de um pacote. Zerado, o pacote é descartado e um pacote de controle (ICMP) é enviado de volta à origem.
  - Protocol: Indica o protocolo que está sendo transportado na parte de dados. IP (0), ICMP(1), TCP(6), etc.
  - Header Cheksum: verifica a correção do cabeçalho;
  - Destination e Source Address: Contêm os endereços IP do nó destino e origem do pacote;
  - Options: campo de tamanho variável (múltiplos de 4 bytes), destinado para experimentações.

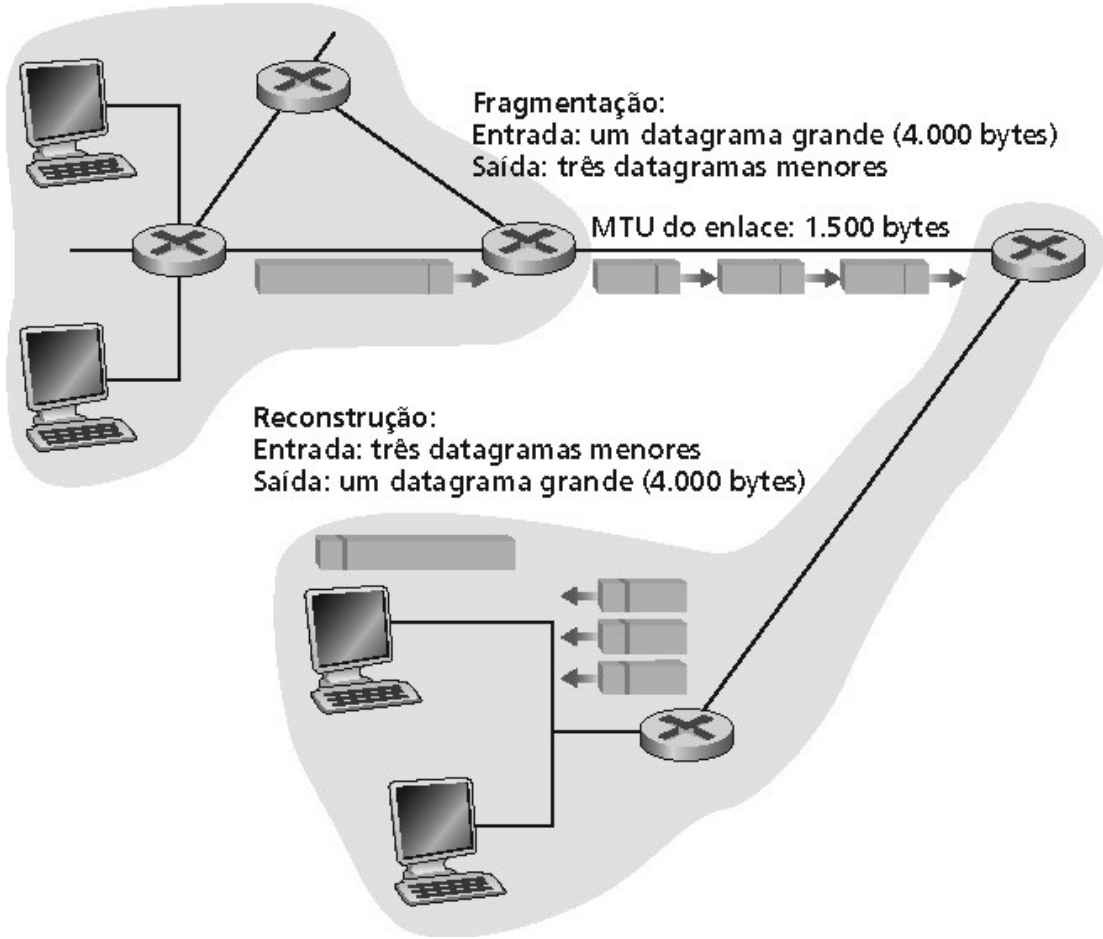
Fragmentação do Datagrama IP

- Vimos na camada de enlace que os links entre hosts variam enquanto tecnologia, taxa de transferência, etc;
  - A quantidade máxima de dados que um quadro da camada de enlace pode carregar é denominada unidade máxima de transmissão (Maximum transmission unit – MTU)

- Como cada datagrama IP é encapsulado dentro do quadro de camada de enlace, a MTU do protocolo de camada de enlace estabelece um limite estrito para o comprimento de um datagrama IP;
  - Em outras palavra, pode ser exigida a fragmentação do datagrama IP

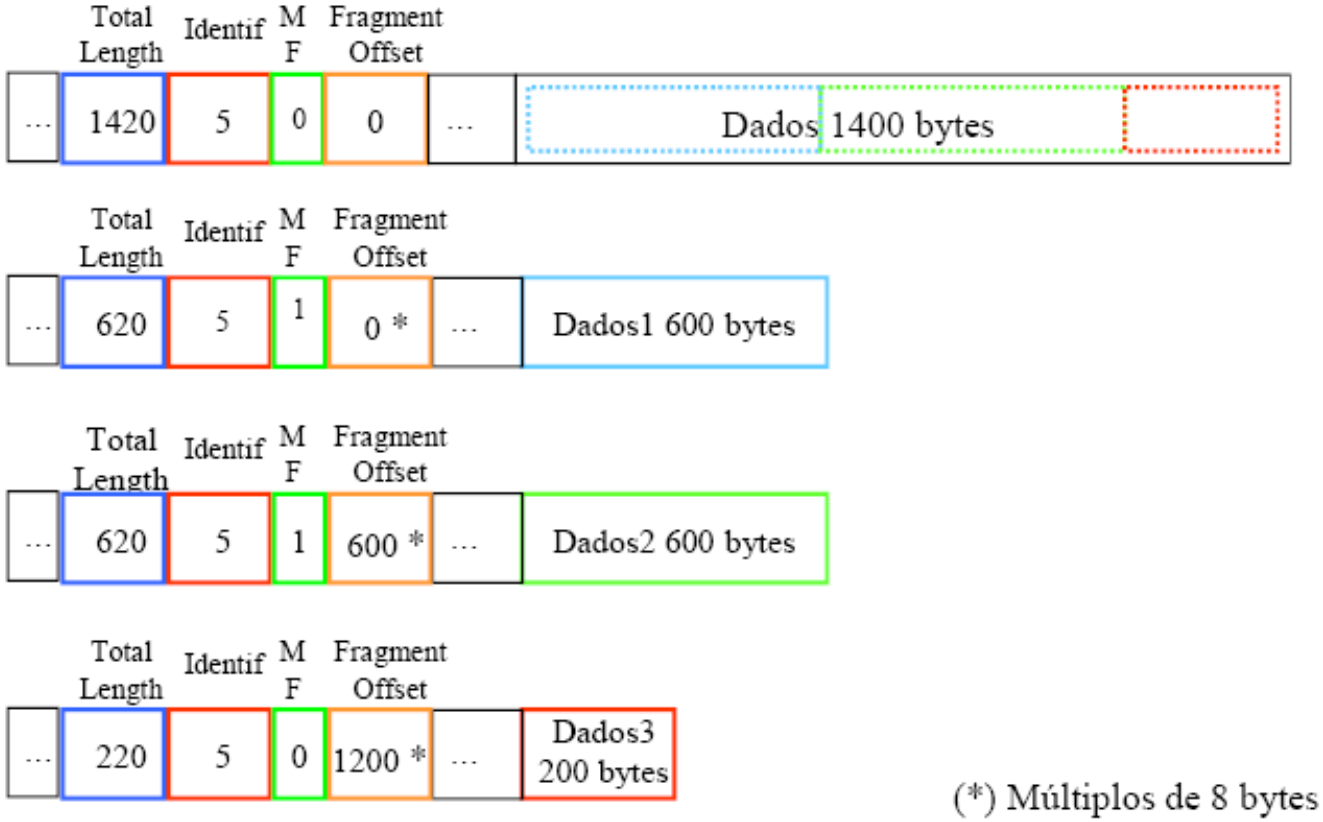
Fragmentação do Datagrama IP

- Vejamos um exemplo de fragmentação e reconstrução do datagrama IP:



Fragmentação do Datagrama IP

- Um outro exemplo, visto a partir do cabeçalho do IPv4:

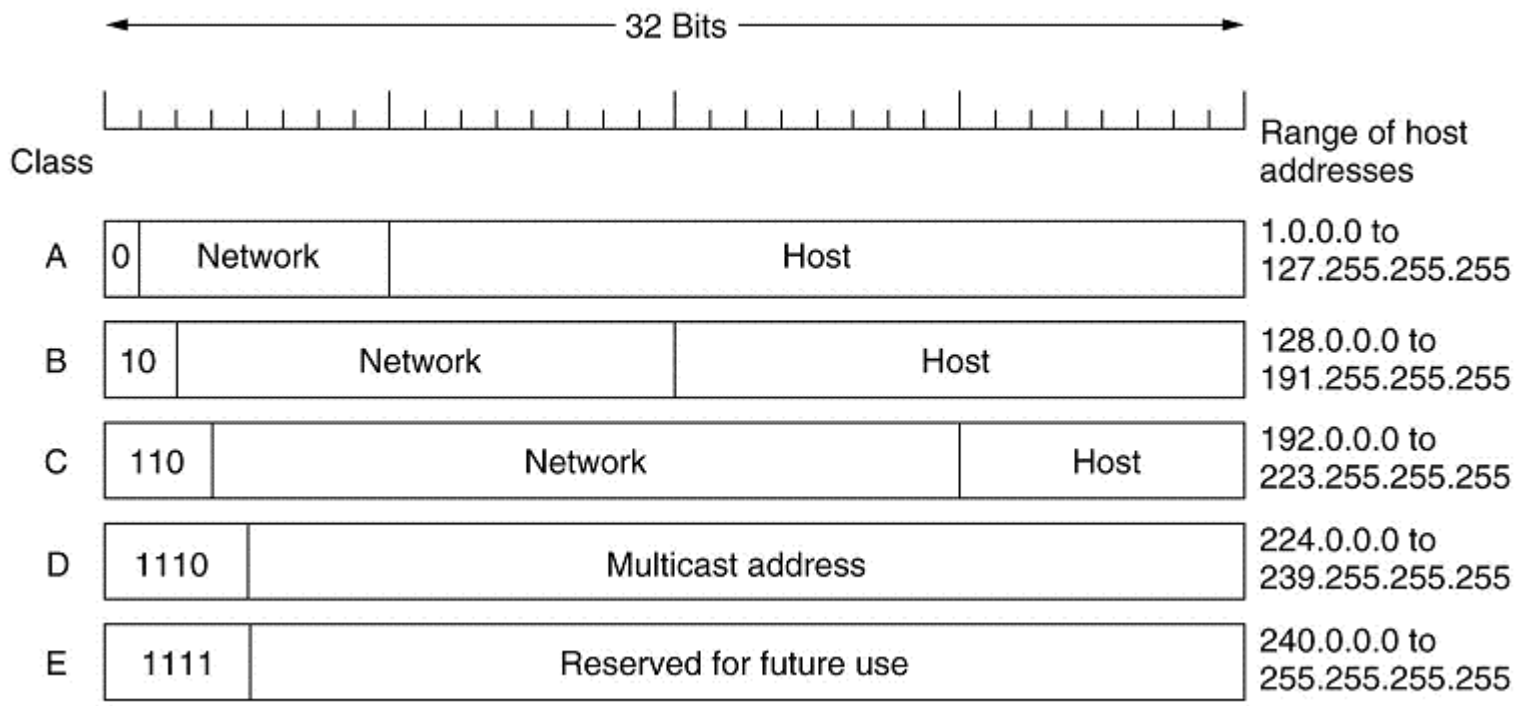


Endereço IP

- Como vimos no cabeçalho do IPv4, existe dois campos reservados para o endereço do emissor e do destinatário;
  - 32 bits (4 bytes);
  - Endereço contém identificação de uma rede e de uma máquina nesta rede;
  - Estações com duas ou mais conexões físicas requerem múltiplos endereços IP (normalmente, um endereço por interface);
  - Endereços podem ser dos tipos: (i) Unicast: indicam uma única máquina na rede; (ii) Broadcast: indicam todas as máquinas numa rede ou (iii) Multicast: usado para comunicação em grupo

Endereço IP

- Classes de Endereços IPs:

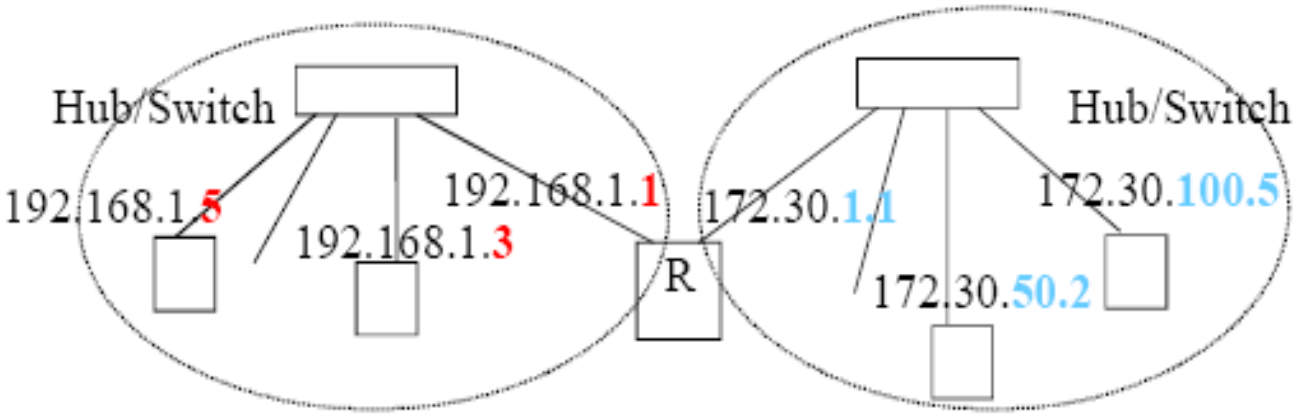


Endereço IP

- Cada endereço Classe A pode ser usado numa rede com 256^3 – 2 máquinas (16.777.214)
  - Endereço que tem valor 0 em todos os bits da porção que indica a máquina na rede é reservado para fazer referência à rede como um todo;
  - Endereço que tem valor 1 em todos os bits da porção que indica a máquina na rede é utilizado para braodcast;
- Endereços Classe B servem a redes com até 256^2 – 2 máquinas (65.534)
- Numa rede Classe C podem ser endereçadas até 254 máquinas

Endereçamento IP

- Exemplo de endereçamento:



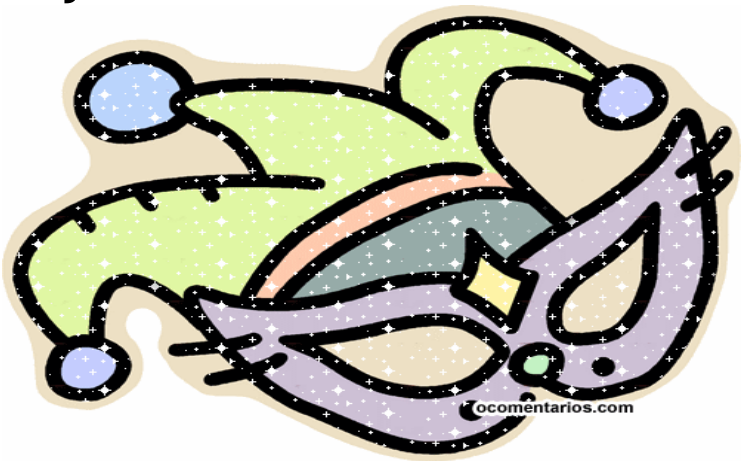
Rede: 192.168.1.0
Máscara: 255.255.255.0
Broadcast: 192.168.1.255
Gateway: 192.168.1.1

Rede: 172.30.0.0
Máscara: 255.255.0.0
Broadcast: 172.30.255.255
Gateway: 172.30.1.1

Sub-redes

- Para implementar a divisão em sub-redes, o roteador principal precisa de uma máscara de sub-rede;

- A máscara de rede indica a divisão entre o número de rede + sub-rede e o host, veja:



Sub-redes

- 1 bit a mais na máscara de uma rede classe C:

Rede original: 192.168.1.0 / Máscara 255.255.255.0

Nova Máscara: 25 bits 11111111.11111111.11111111.10000000
255. 255. 255. 128

Novas redes: 192.168.1.00000000 - 192.168.1.0
192.168.1.10000000 - 192.168.1.128

Rede 1: 192.168.1.0
Máscara: 255.255.255.128 ou /25
Endereços: 192.168.1.00000001 (1) até 192.168.1.01111110 (126)
Broadcast: 192.168.1.01111111 (127)

Rede 2: 192.168.1.128
Máscara: 255.255.255.128 ou /25
Endereços: 192.168.1.10000001 (129) até 192.168.1.11111110 (254)
Broadcast: 192.168.1.11111111 (255)

Sub-redes

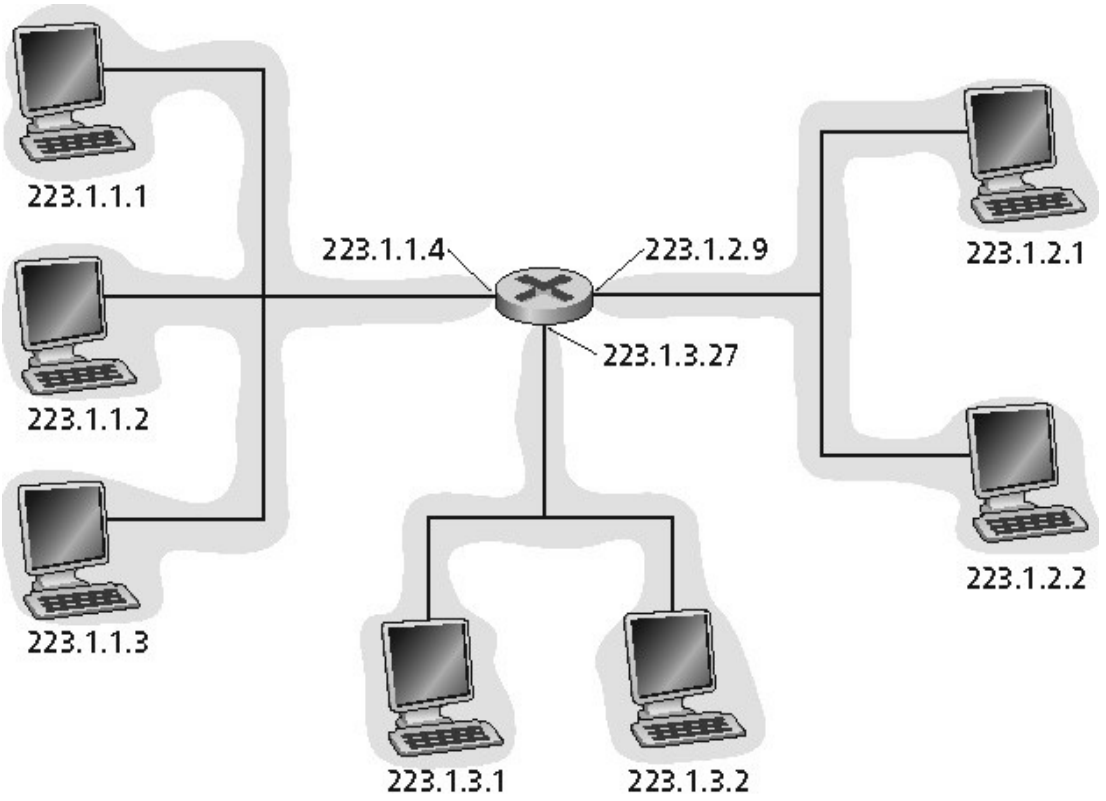
- Exemplo de segmentação:

Rede	máscara (bits)	broadcast	faixa de IPs
192.168.1.0	255.255.255.192 (26)	192.168.1.63	192.168.1.1-62
192.168.1.64	255.255.255.192 (26)	192.168.1.127	192.168.1.65-126
192.168.1.128	255.255.255.192 (26)	192.168.1.191	192.168.1.129-190
192.168.1.192	255.255.255.192 (26)	192.168.1.255	192.168.1.193-254

Rede	máscara (bits)	broadcast	faixa de IPs
192.168.1.0	255.255.255. 224 (27)	192.168.1.31	192.168.1.1-30
192.168.1.32	255.255.255. 224 (27)	192.168.1.63	192.168.1.33-62
192.168.1.64	255.255.255. 224 (27)	192.168.1.95	192.168.1.65-94
192.168.1.96	255.255.255. 224 (27)	192.168.1.127	192.168.1.97-126
192.168.1.128	255.255.255. 224 (27)	192.168.1.159	192.168.1.128-158
192.168.1.160	255.255.255. 224 (27)	192.168.1.191	192.168.1.161-190
192.168.1.192	255.255.255. 224 (27)	192.168.1.223	192.168.1.193-222
192.168.1.224	255.255.255. 224 (27)	192.168.1.255	192.168.1.225-254

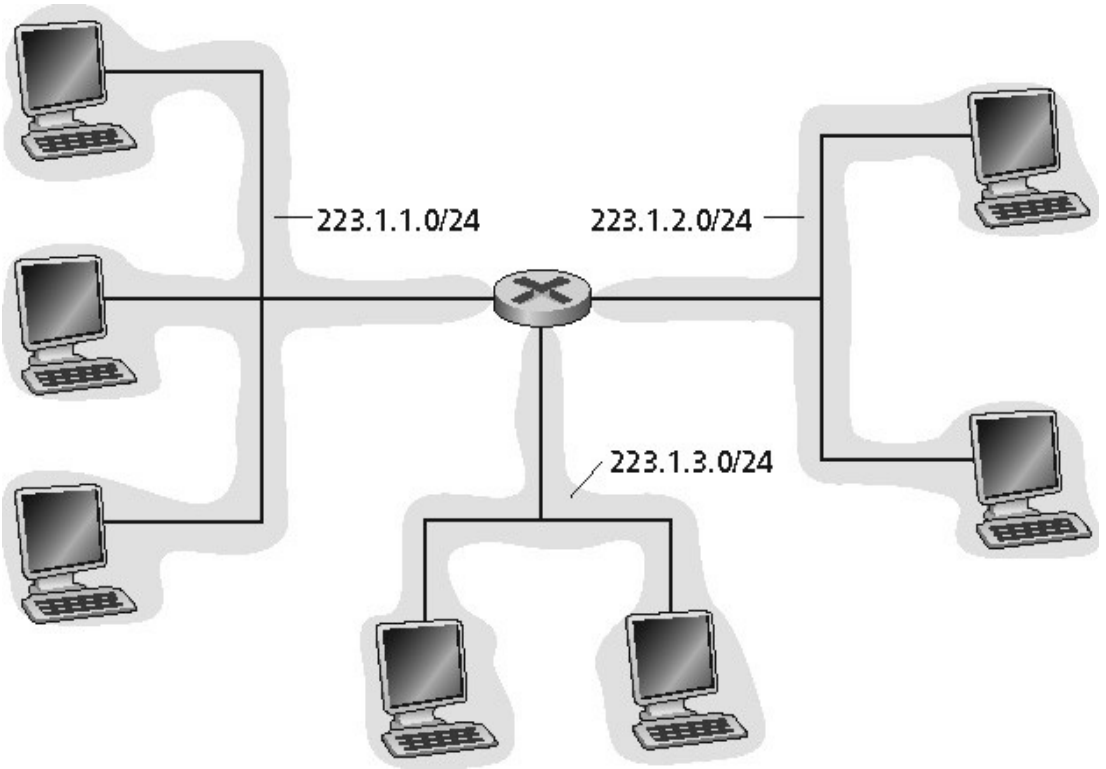
Sub-redes

- Para entendermos melhor como as sub-redes funcionam, é necessário explicar como os pacotes IP são processados em um roteador;



Sub-redes

- Quando a divisão em su-redes é introduzida, um roteador da sub-rede x sabe como alcançar todas as outras sub-redes mas nã conhece detalhes dobre os hosts de outras sub-redes;



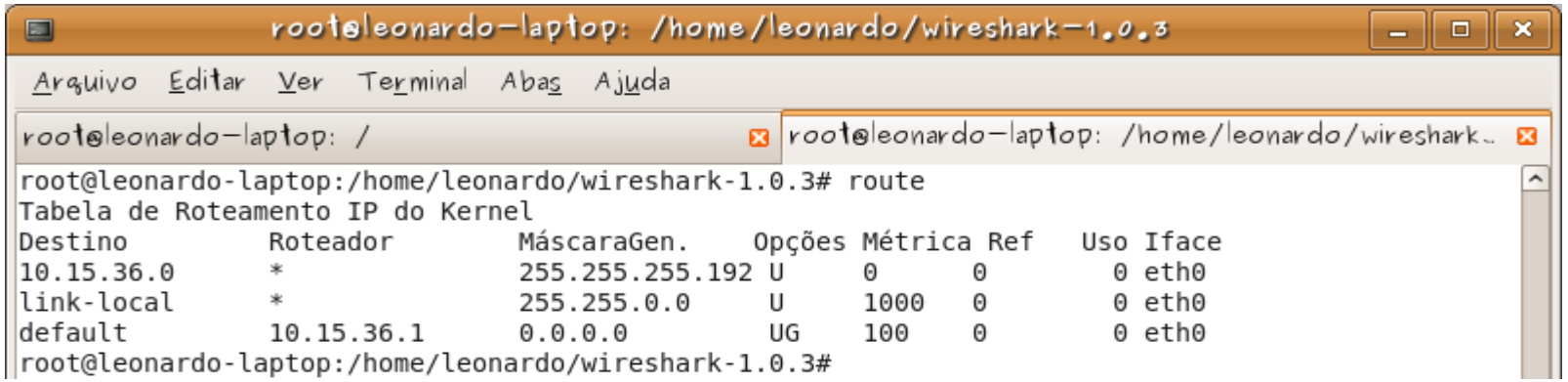
Sub-redes

- Na realidade, a única modificação é fazer com que cada roteador seja submetido a um AND booleano com a máscara de sub-rede, a fim de eliminar o número de host e pesquisa o endereço resultante em suas tabelas;
  - Roteamento pode ser feito a partir de tabela fixas, ou baseado em informações dinâmicas do estado da rede e de suas conexões;

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
200.18.99.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	200.18.99.1	0.0.0.0	UG	1	0	0	eth0

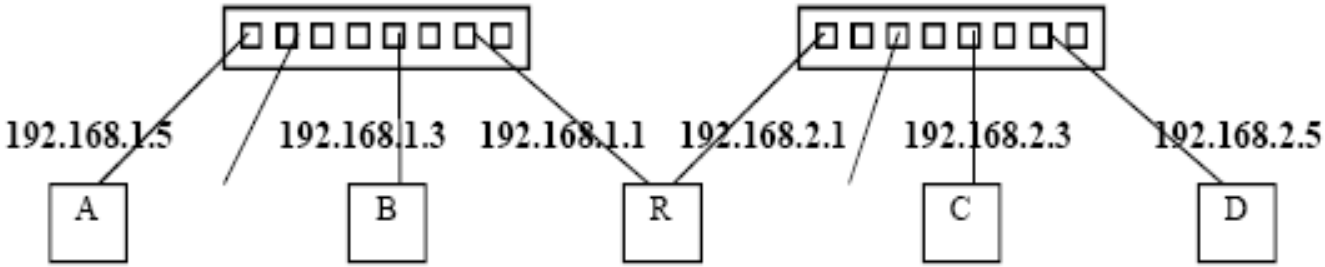
Sub-redes

- Tabela de rota, presente em todas as máquina, contém:
  - Endereço IP do destino da rota (host, rede ou default)
  - Endereço IP do intermediário para entrega do pacote
  - Flags: destino (host, rede) status (ativa, ou não), tipo (dinâmica ou estática), modificação (protocolos dinâmico)
  - Métrica distância até o destino (saltos)
  - Identificação da interface de rede a ser utililizada.



Sub-redes

- Encaminhamento de pacote: Transmissão na rede interna



Transmissão A – B

				Orig: A	Dest: B			
Pacote IP:				...	192.168.1.5	192.168.1.3	Info	
	Dest	Orig						
Quadro Ethernet:	MAC B	MAC A	0800	...	192.168.1.5	192.168.1.3	Info	FCS

Sub-redes

- Para cada entrada na tabela de rotas, ou até que seja encontrado um caminho:
  - Se ((endereço destino & netmask da rota) == endereço da rota)
  - Então envia pacote encapsulado em quadro de rede para o gateway da rota através da interface especificada

Ex.: IP: 200.18.99.238

máscara: 255.255.255.0

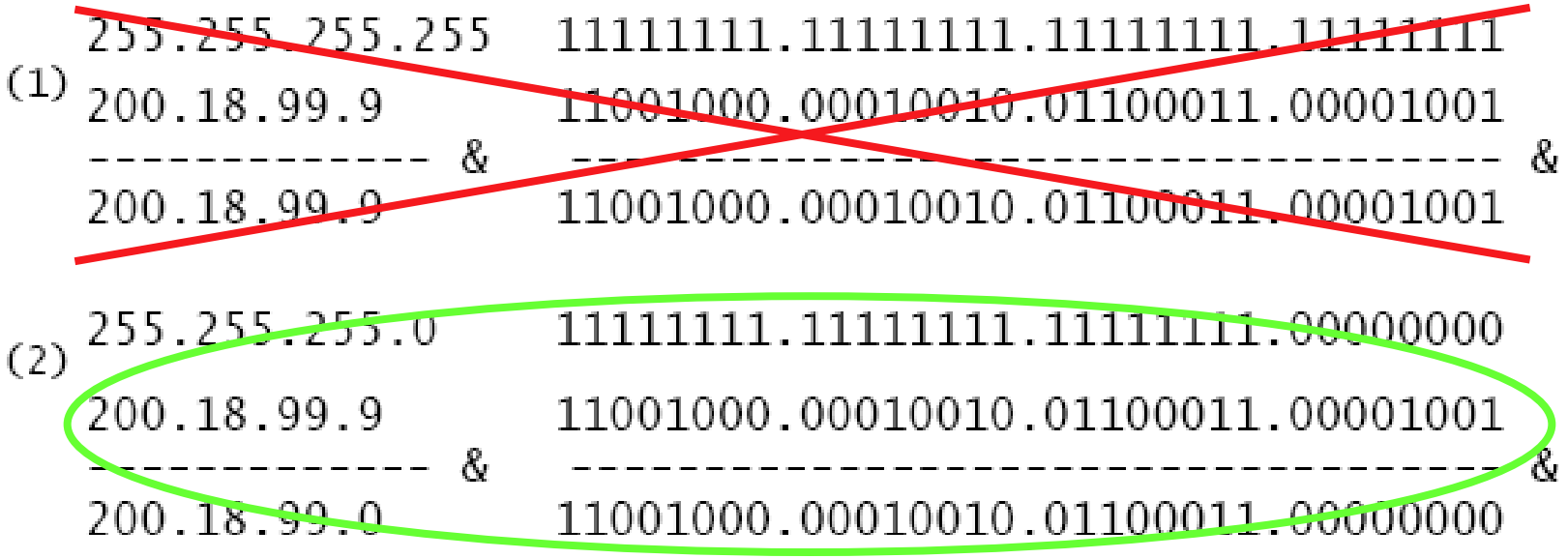
Gateway: 200.18.99.1

rotas:	destino	máscara	gateway	interface
(1)	200.18.99.238	255.255.255.255	200.18.99.238	200.18.99.238
(2)	200.18.99.0	255.255.255.0	200.18.99.238	200.18.99.238
(3)	0.0.0.0	0.0.0.0	200.18.99.1	200.18.99.238

Destino: 200.18.99.9

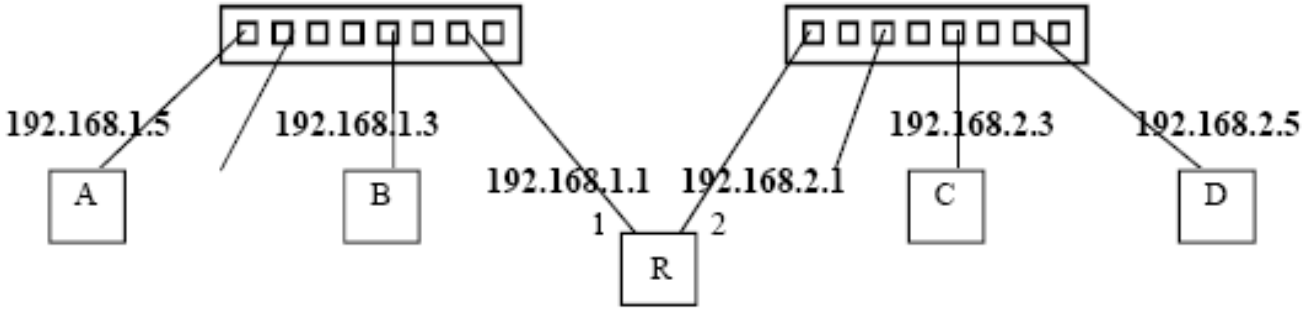
Sub-redes

- Verificação de endereços:



Sub-redes

- Encaminhamento de pacote: Transmissão na rede externa



Transmissão A – C

				Orig: A	Dest: C			
Pacote IP:				...	192.168.1.5	192.168.2.3	Info	
	Dest	Orig						
Quadro Ethernet:	MAC R1	MAC A	0800	...	192.168.1.5	192.168.2.3	Info	FCS
	Dest	Orig						
Quadro Ethernet:	MAC C	MAC R2	0800	*	192.168.1.5	192.168.2.3	Info	FCS

*: Necessário decrementar TTL e recalcular checksum do cabeçalho

Sub-redes

- Verificação de endereços:

Ex.: IP: 200.18.99.238; máscara: 255.255.255.0; Gateway: 200.18.99.1

rotas:	destino	máscara	gateway	interface
(1)	200.18.99.238	255.255.255.255	200.18.99.238	200.18.99.238
(2)	200.18.99.0	255.255.255.0	200.18.99.238	200.18.99.238
(3)	0.0.0.0	0.0.0.0	200.18.99.1	200.18.99.238

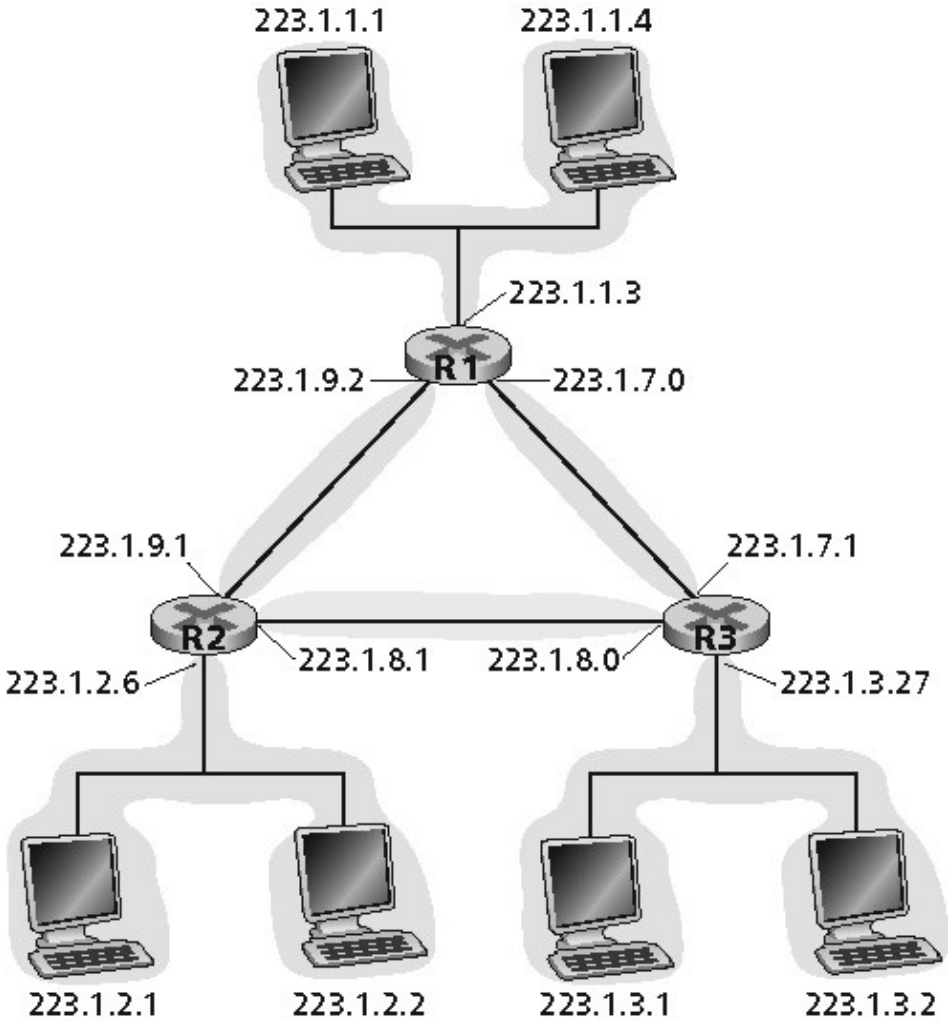
Destino: 200.1.2.5

(2)
```
255.255.255.0      11111111.11111111.11111111.00000000
200.1.2.5          11001000.00000001.00000010.00000101
------------- &    ---------------------------------- &
200.1.2.0          11001000.00000001.00000010.00000000
```

(3)
```
0.0.0.0            00000000.00000000.00000000.00000000
200.1.2.5          11001000.00000001.00000010.00000101
------------- &    ---------------------------------- &
0.0.0.0            00000000.00000000.00000000.00000000
```

Sub-redes

- Entendeu sub-redes? Então responda, quantas sub-redes existe na figura ao lado:
  - Para determinar as sub-redes, destaque cada interface de seu hospedeiro ou roteador, criando ilhas de redes isoladas. Cada rede isolada é considerada uma sub-rede



Sub-redes

- Estrutura hierárquica de roteamento aliada ao crescimento da Internet gerou tabelas de rotas muito grandes em nós que concentram tráfego (teoria das filas);
- Idéia: roteamento baseado no endereçamento e no número de bits da máscara;
- Possibilidade de agrupar endereços de rede, atribuindo endereços consecutivos para uma mesma região da rede;

Sub-redes

- Resultado: redução das tabelas de roteamento
  - End. 194.0.0.0 a 195.255.255.255 – Europa
  - End. 198.0.0.0 a 199.255.255.255 – A. Norte
  - End. 200.0.0.0 a 201.255.255.255 – A. Central e do Sul
  - End. 202.0.0.0 a 203.255.255.255 – Ásia e Pacífico

- Independentemente da classe de endereço utilizada, o uso da máscara de rede permite segmentação de redes em redes menores;

- Máscaras de rede indica quantos bits são utilizados para a identificação da rede e quantos para os hosts;

CIDR – Classes Interdomain Routing

- Essa estratégia é conhecida como Roteamento Interdomínio sem Classes (pronuncia cidra em inglês) [RFC 1519];
  - O endereçamento de sub-redes tem a forma decimal com pontos de separação a.b.c.d/x, em que o x indica o número de bits existentes na primeira parte do endereço;
  - Os x bits mais significativos constituem a parcela da rede do endereço IP e normalmente são denominados prefixo;

200.23.16.0/23

NAT – Network Address Translation

- O problema de esgotar endereços IP não é um problema teórico que pode ocorrer em um futuro distante, ele está acontecendo aqui e agora:
  - Grande número de máquinas nas empresas ligadas 24 horas;
  - Aumento do número usuários de ADSL;
  - Má distribuição dos endereços IP no início da Internet;

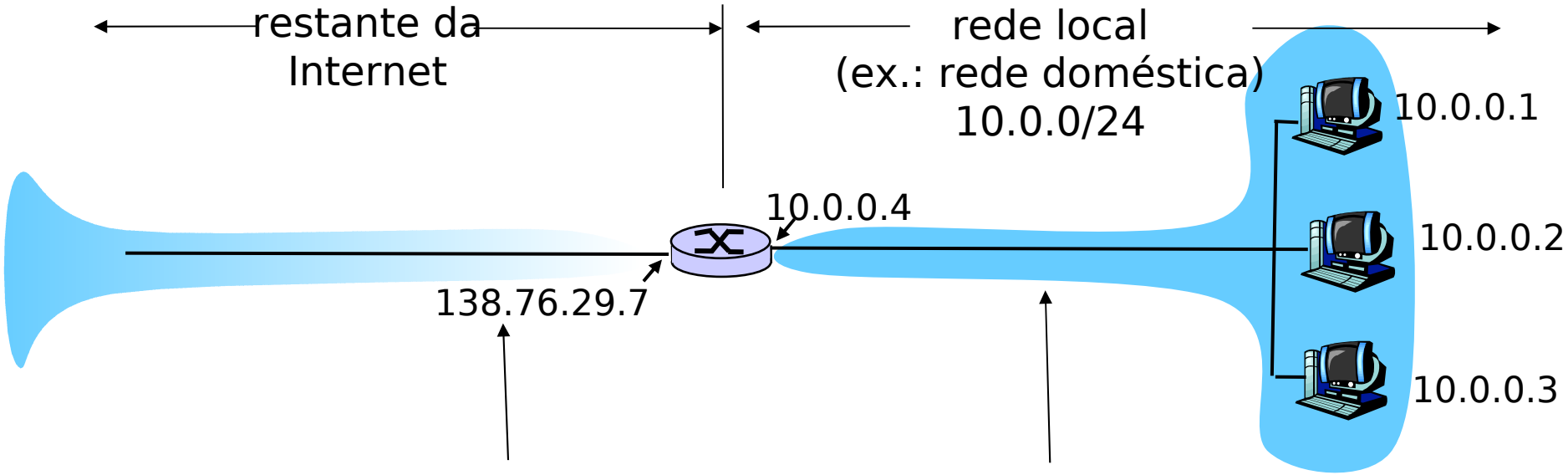
- Solução:
  - Migração para o Ipv6 (128 bits de endereçamento)
  - NAT [RFC 2663; RFC 3022]

NAT – Network Address Translation

- A idéia é atribuir apenas 1(um) IP válido às empresas para tráfego na Internet;
- Dentro da empresa, todo computador obtém um endereço IP exlusivo, usado para roteamento do tráfego interno;
- Porém, quando um pacote sai da empresa e vai para o ISP, ocorre uma conversão de endereço;

NAT – Network Address Translation

- Operação do NAT:



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 10.0.0/24 para origem, destino (usualmente)

NAT – Network Address Translation

- Para tornar esse esquema possível, três intervalos de endereços IP foram declarados como privativos:
  - 10.0.0.0 - 10.255.255.255/8 (16.777.216 hosts)
  - 172.16.0.0 - 172.31.255.255/12 (1.048.576 hosts)
  - 192.168.0.0 - 192.168.255.255/16 (65.536 hosts)

- As empresas podem utilizá-los internamente como desejarem:
  - A única regra é que nenhum pacote contendo esses endereços pode aparecer na própria Internet;

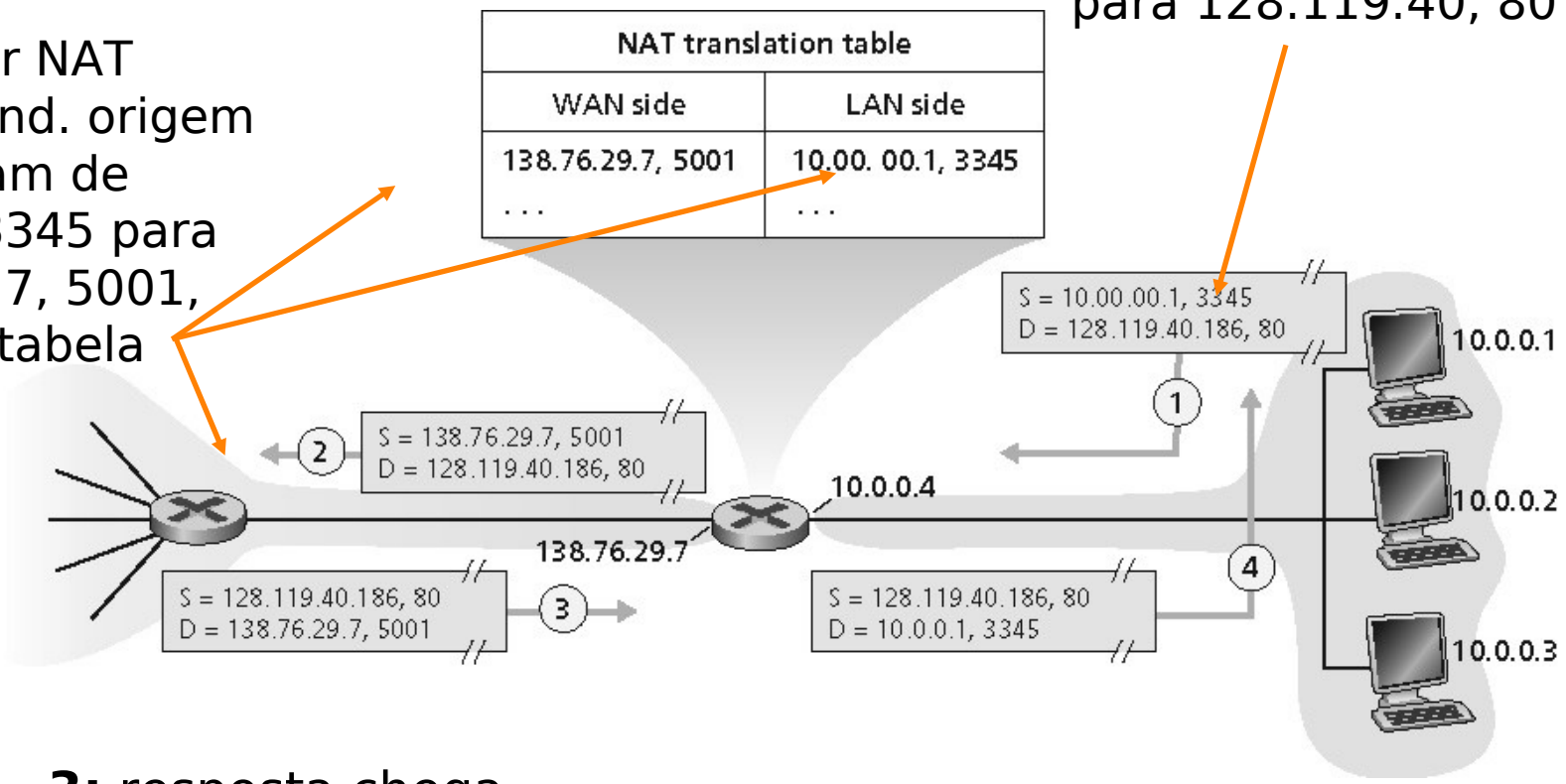
NAT – Network Address Translation

- Implementação: o roteador NAT deve:
  - **Datagramas que saem: substituir** (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.
  - **Lembrar (na 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: substituir** (endereço IP do NAT, nova porta #) nos campos de destino de cada datagrama pelos correspondentes (endereço IP de origem, porta #) armazenados da tabela NAT

NAT – Network Address Translation

1: hospedeiro 10.0.0.1 envia datagrama para 128.119.40, 80

2: roteador NAT substitui end. origem do datagram de 10.0.0.1, 3345 para 138.76.29.7, 5001, atualiza a tabela



3: resposta chega endereço de destino: 138.76.29.7, 5001

NAT – Network Address Translation

- Campo número de porta com 16 bits:
  - 60.000 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 possilidade de NAT deve ser levada em conta pelos desenvolvedores de aplicações, ex., aplicações P2P
  - A escassez de endereços deveria ser resolvida pelo IPv6

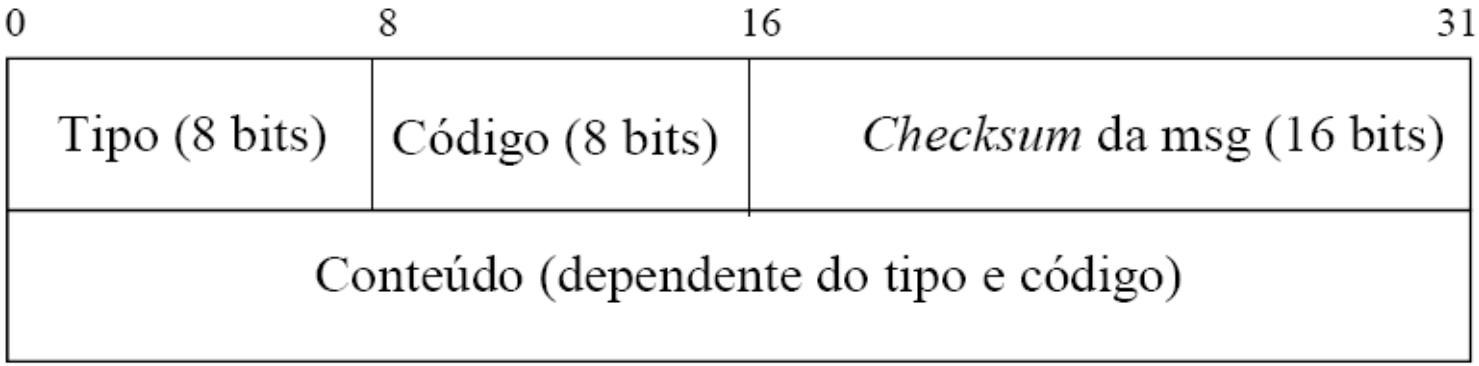
ICMP – Internet Control Message Protocol

- O ICMP, especificado no RFC 792, é usado por hospedeiros e roteadores para comunicar informações de camada de rede entre si;

- A utilização mas comum do ICMP é para comunicação de erros:
  - Em algum ponto, um roteador não conseguiu descobrir um caminho para o hospedeiro especificado em usa aplicação (HTTP, por exemplo)
  - Mensagens ICMP têm um campo de tipo e um campo de código;

ICMP – Internet Control Message Protocol

- Além, disso contém o cabeçalho e os primeiros 8 bytes do datagrama IP que causou a criação da mensagem ICMP em primeiro lugar, veja:



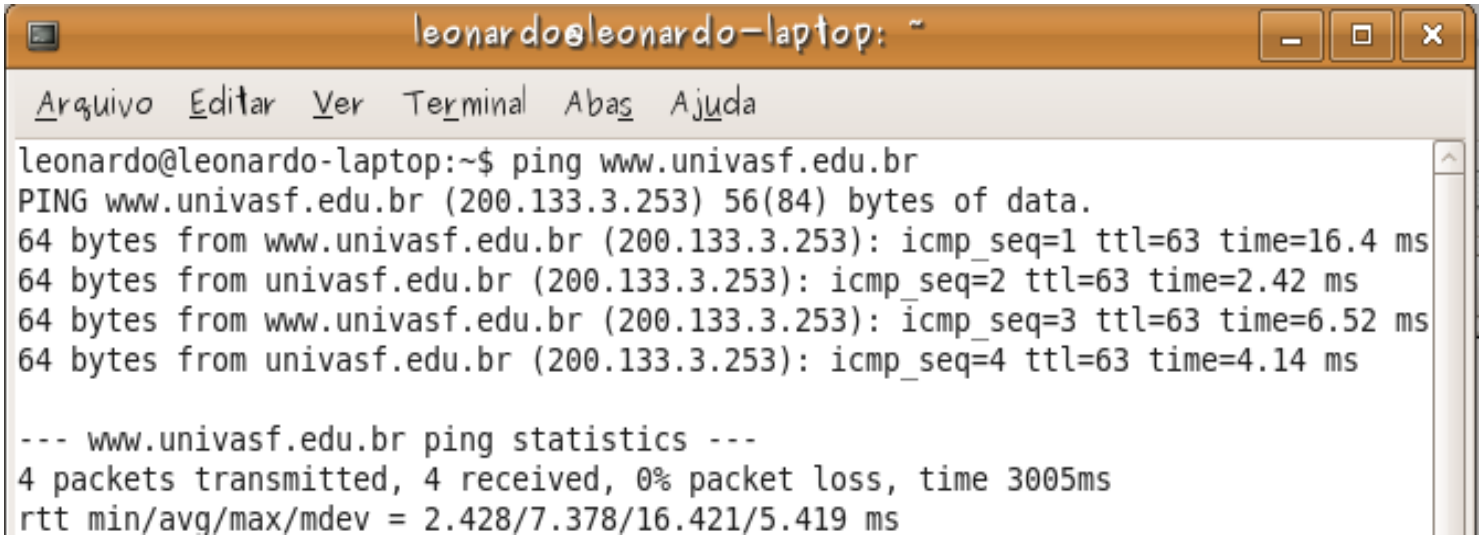
ICMP – Internet Control Message Protocol

- Veja os tipos de mensagens ICMP:

Tipo	Código	Descrição	Query	Error
0	0	*Echo reply (ping reply)*	*	
3		*Destination unreachable*		*
	0	*Network unreachable*		*
	1	*Host unreachable*		*
	2	*Protocol unreachable*		*
	3	*Port unreachable*		*
	4	*Fragmentation needed but DF bit set*		*
	6	*Destination network unknown*		*
	7	*Destination host unknown*		*
	11	*Network unreachable for type of service*		*
	12	*Host unreachable for type of service*		*
8	0	*Echo request (ping request)*	*	

ICMP – Internet Control Message Protocol

- Exemplo:
  - O programa ping, envia uma mensagem ICMP do tipo 8 código 0 para o hospedeiro específico;
  - O hospedeiro de destino, ao ver a solicitação de echo, devolve uma resposta eco ICMP do tipo 0 código 0



IPv6

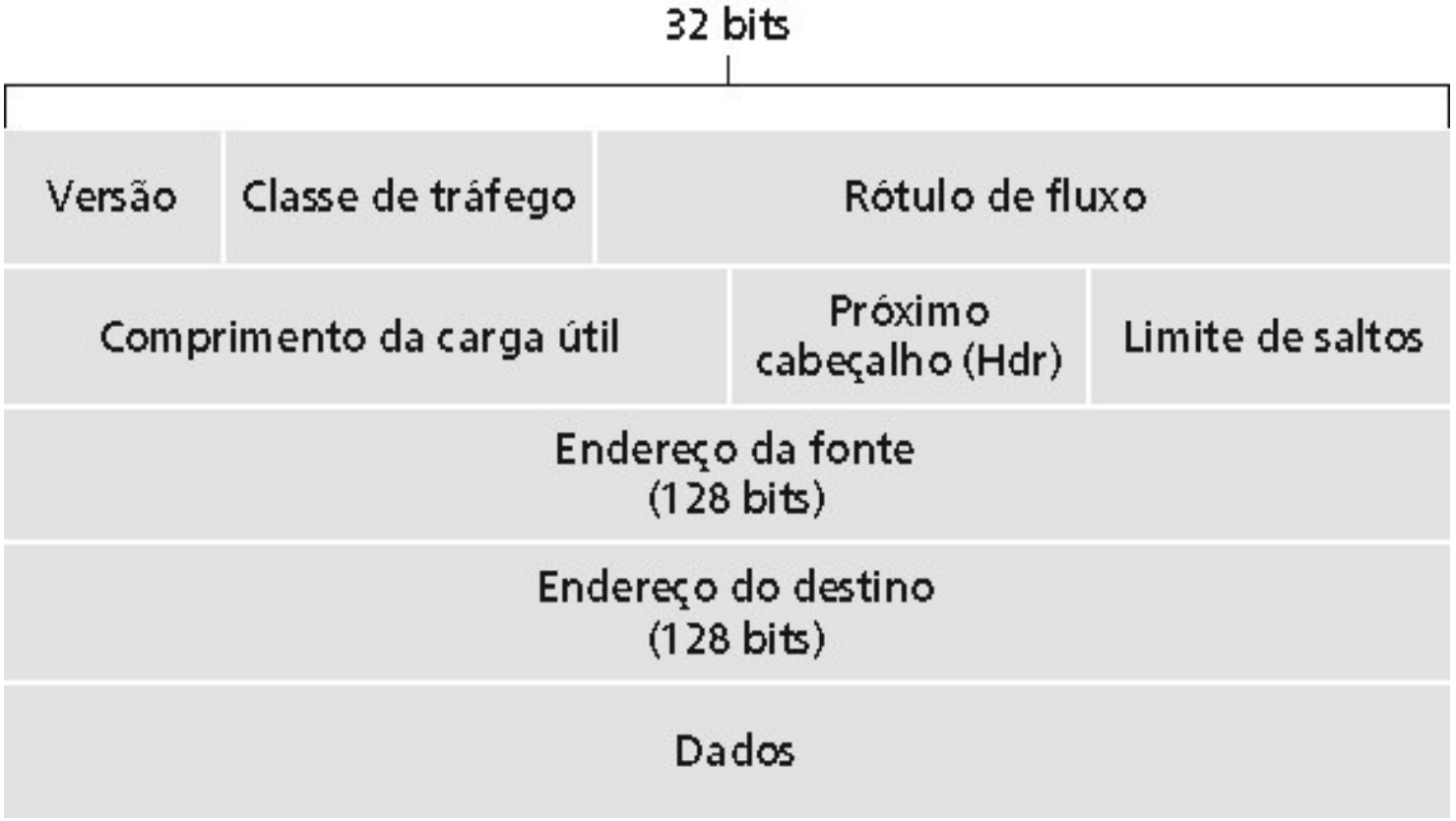
- Motivação inicial: o espaço de endereços de 32 bits está próximo de ser completamente alocado

- Motivação adicional:
  - Melhorar o formato do header para permitir maior velocidade de processamento e de transmissão
  - Mudanças no header para incorporar mecanismos de controle de QoS

- Formato do datagrama Ipv6 [RFC 2460]:
  - Cabeçalho fixo de 40 bytes
  - Não é permitida fragmentação

IPv6

- Cabeçalho do datagrama IPv6:



IPv6

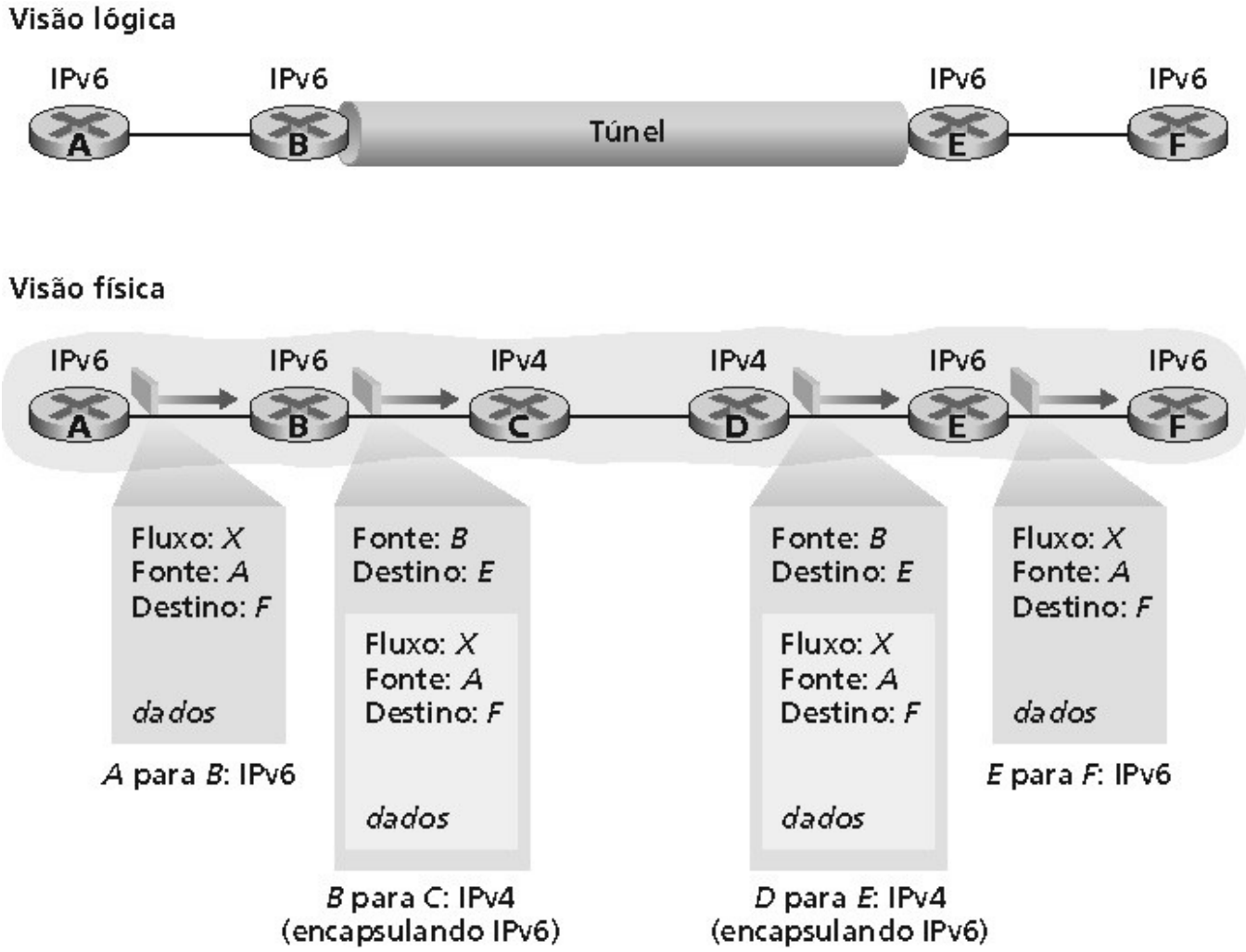
- Considerações:
  - Priority: permitir definir prioridades diferenciadas para vários fluxos de informação
  - Flow label: identifica datagramas do mesmo “fluxo.” (conceito de “fluxo” não é bem definido).
  - Next header: identifica o protocolo da camada superior ou um header auxiliar
  - checksum: removido inteiramente para reduzir o tempo de processamento em cada salto
  - Options: são permitidas, mas são alocadas em cabeçalhos suplementares, indicados pelo campo “Next header”
  - ICMPv6: nova versão de ICMP

IPv6

- Aceita bilhões de hosts
- Reduz o tamanho das tabelas de roteamento
- Possibilita que o pacote seja processado com mais rapidez
- Oferece mais segurança (autenticação e privacidade)
- Tipo de serviço (tempo real, por exemplo)
- Funções de gerenciamento de grupos multicast
- Nem todos os roteadores poderão ser atualizados simultaneamente
- Não haverá um dia da vacinação
- Como a rede irá operar com roteadores mistos de IPv4 e IPv6?
- **Tunelamento**: IPv6 transportado dentro de pacotes IPv4 entre roteadores IPv4

IPv6

- Tunelamento:



Bibliografia

- TANENBAUM, A.S.: *Redes de Computadores,* Elsevier, Rio de Janeiro: 2003.

- KUROSE, J.F e ROSS, K.W.: *Computer Networking third edition a top-down approach featuring the Internet,* 3 ed, São Paulo: Pearson Addison Wesley, 2006.