CRIPTOGRAFIA

- **Revisão de Camadas de Protocolos**
  - **Estrutura do quadro ethernet;**
  - **Protocolo ARP;**
  - **Protocolos de camada de rede (datagrama, ICMP).**

ESTRUTURA DO QUADRO ETHERNET

- Preâmbulo – corresponde a seqüência padrão de *bits* (10101010) usada de acordo com a codificação Manchester para que o receptor possa sincronizar o relógio com o transmissor.

7	1	6	6	2	46-1500	4
Preâmbulo	Início do delimitador de quadro	Endereço de destino	Endereço da origem	Tipo	Dados	Seqüência de verificação do quadro

ESTRUTURA DO QUADRO ETHERNET

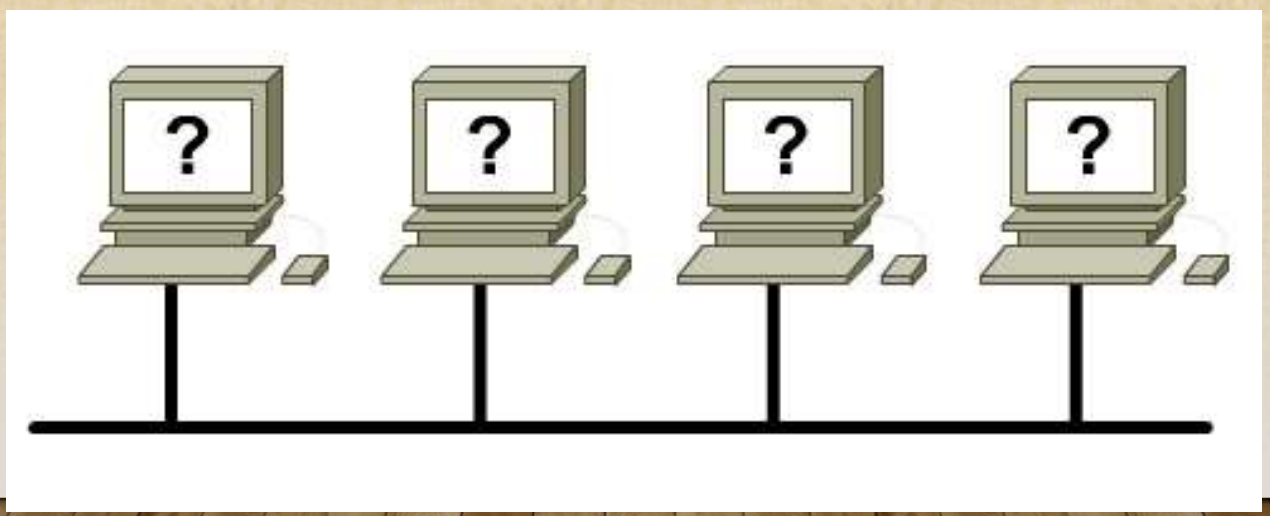
- Início do quadro (SOF, *start-of-frame*) – É gerada uma seqüência (10101011) para gerar início do quadro e habilitar a recepção.
- Endereços de origem e de destino (48 bits) - O endereço de origem é sempre um endereço *unicast* (nó único). O endereço de destino pode ser *unicast* (único nó), *multicast* (grupo), ou *broadcast* (todos os nós).
- Tipo (*Ethernet*) - O tipo especifica o protocolo da camada superior para receber os dados depois que o processamento da *Ethernet* estiver concluído (multiplexa os dados da camada de rede). Pode ser o IP, Novell IPX, etc.

ESTRUTURA DO QUADRO ETHERNET

- Dados (*Ethernet*) – esse campo carrega o datagrama IP. A unidade máxima de transferência (MTU) da *Ethernet* é de 1500 Bytes e a mínima é de 46 Bytes.
- *Frame check sequence* (FCS) - Essa seqüência contém um verificador de redundância cíclica de 4 bytes (CRC), criado pelo dispositivo emissor e recalculado pelo dispositivo de recepção para verificar se há quadros danificados.

ENDERAÇAMENTO MAC

- Sem o endereço MAC, teríamos um conjunto de computadores sem nome na LAN. Portanto, na camada de enlace, um cabeçalho e possivelmente um trailer, são adicionados aos dados da camada superior.



ENDERAÇAMENTO MAC

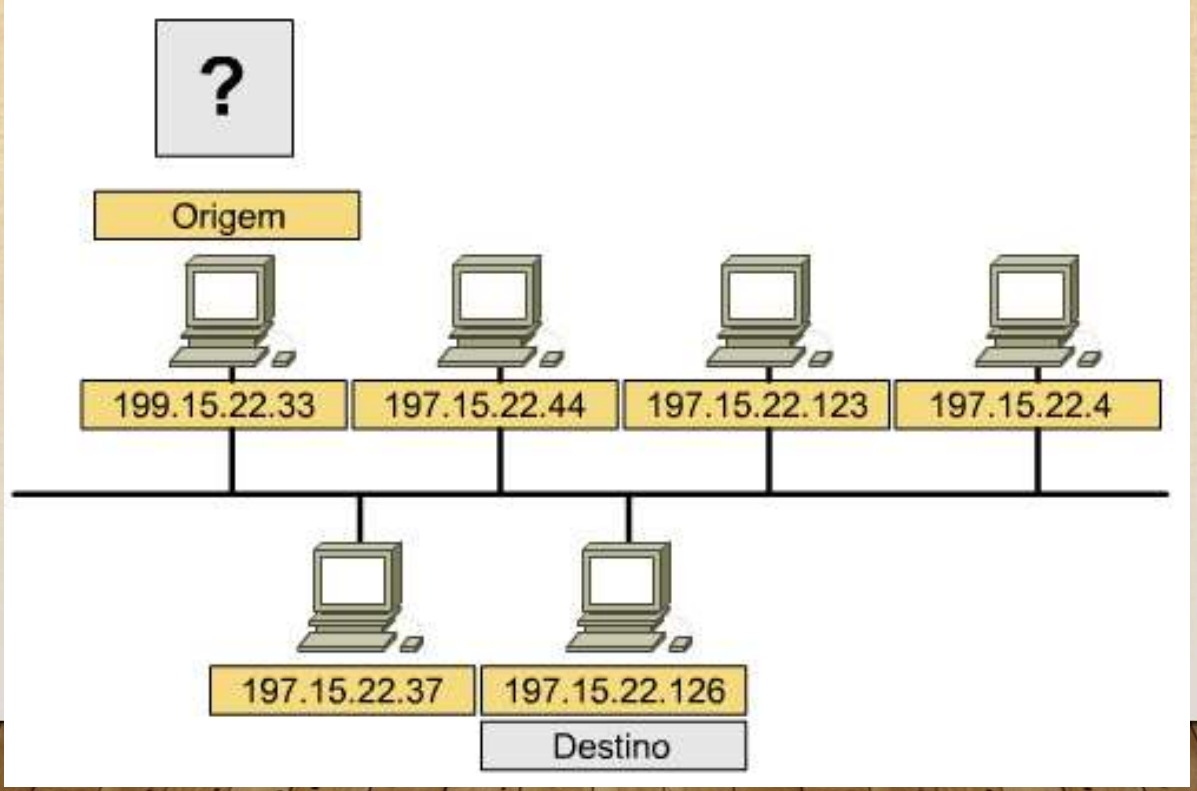
- Todos os computadores têm uma forma exclusiva de se identificar. Cada computador, esteja ou não conectado a uma rede, tem um endereço físico. Nunca dois endereços físicos são iguais (MAC da placa de rede).
- Antes de sair da fábrica, o fabricante do hardware atribui um endereço físico a cada placa de rede. Esse endereço é programado em um chip na placa de rede. Como o endereço MAC está localizado na placa de rede, se a placa de rede fosse trocada em um computador, o endereço físico da estação mudaria para o novo endereço MAC. Os endereços MAC são gravados usando-se números hexadecimais (base 16), por exemplo, 00:BC:0C:12:34:56 (48 bits).

PROTOCOLO ARP

- O ARP (*Address Resolution Protocol*) é responsável pela resolução (tradução) de endereços IP em endereços MAC. Essa resolução é necessária, pois os dispositivos se comunicam somente através dos endereços MAC.

PROTOCOLO ARP

- Processos de resolução de ARP:
  - O protocolo IP solicita ao ARP a conversão de um endereço IP para o endereço MAC;



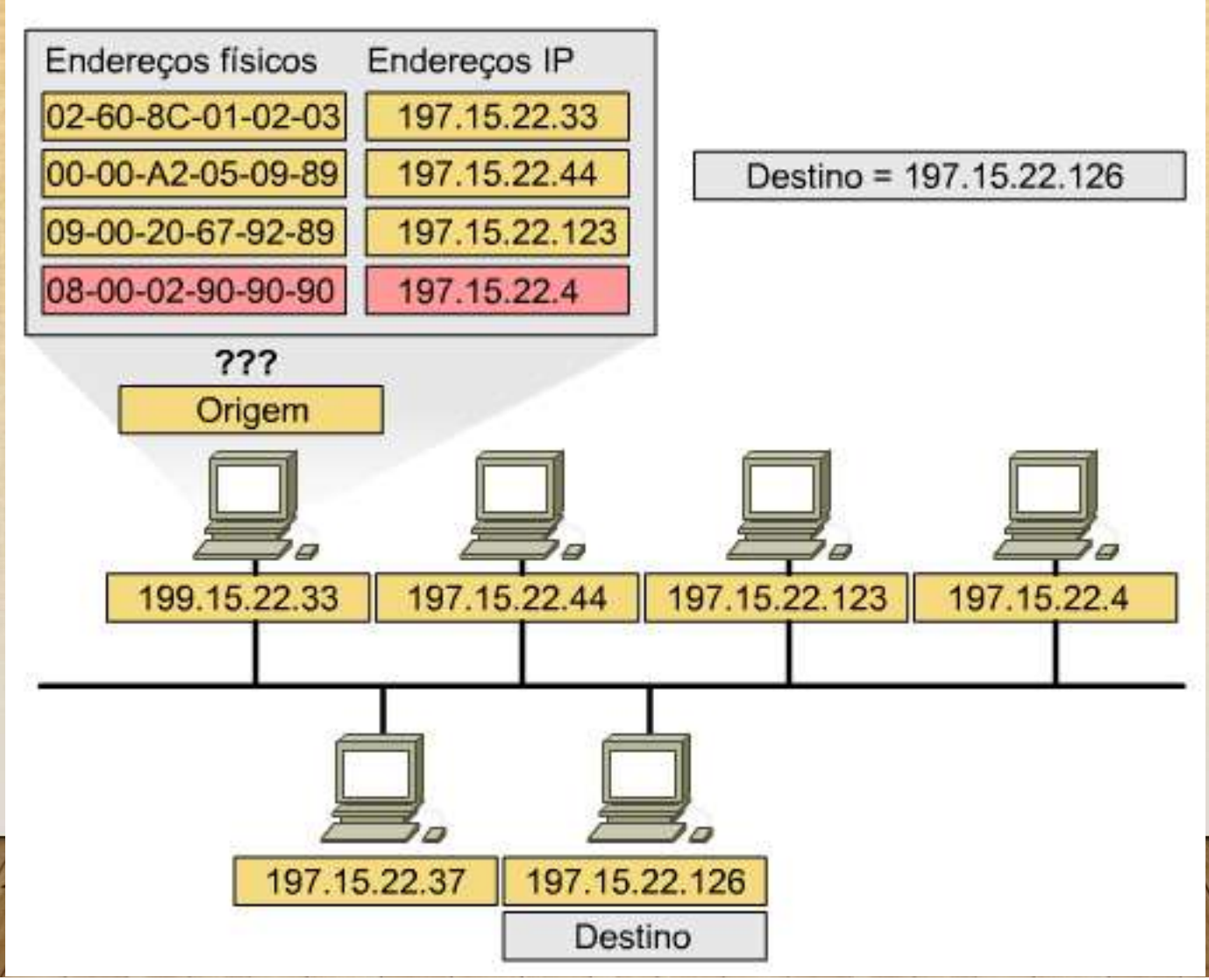
PROTOCOLO ARP

- Processos de resolução de ARP:
  - O protocolo ARP envia uma mensagem do tipo *broadcast* requisitando o endereço MAC (*Arp Request*);

PROTOCOLO ARP

- Processos de resolução de ARP:
  - Todas as máquinas da rede recebem essa mensagem e comparam com o endereço IP solicitado com o próprio endereço;
  - A máquina cujo endereço IP for igual ao solicitado enviará uma mensagem de resposta (ARP *Reply*);
  - O protocolo ARP recebe essa mensagem contendo o endereço físico da máquina configurada com o endereço IP solicitado, que será utilizado para a transmissão do pacote.

PROTOCOLO ARP



PROTOCOLO ARP

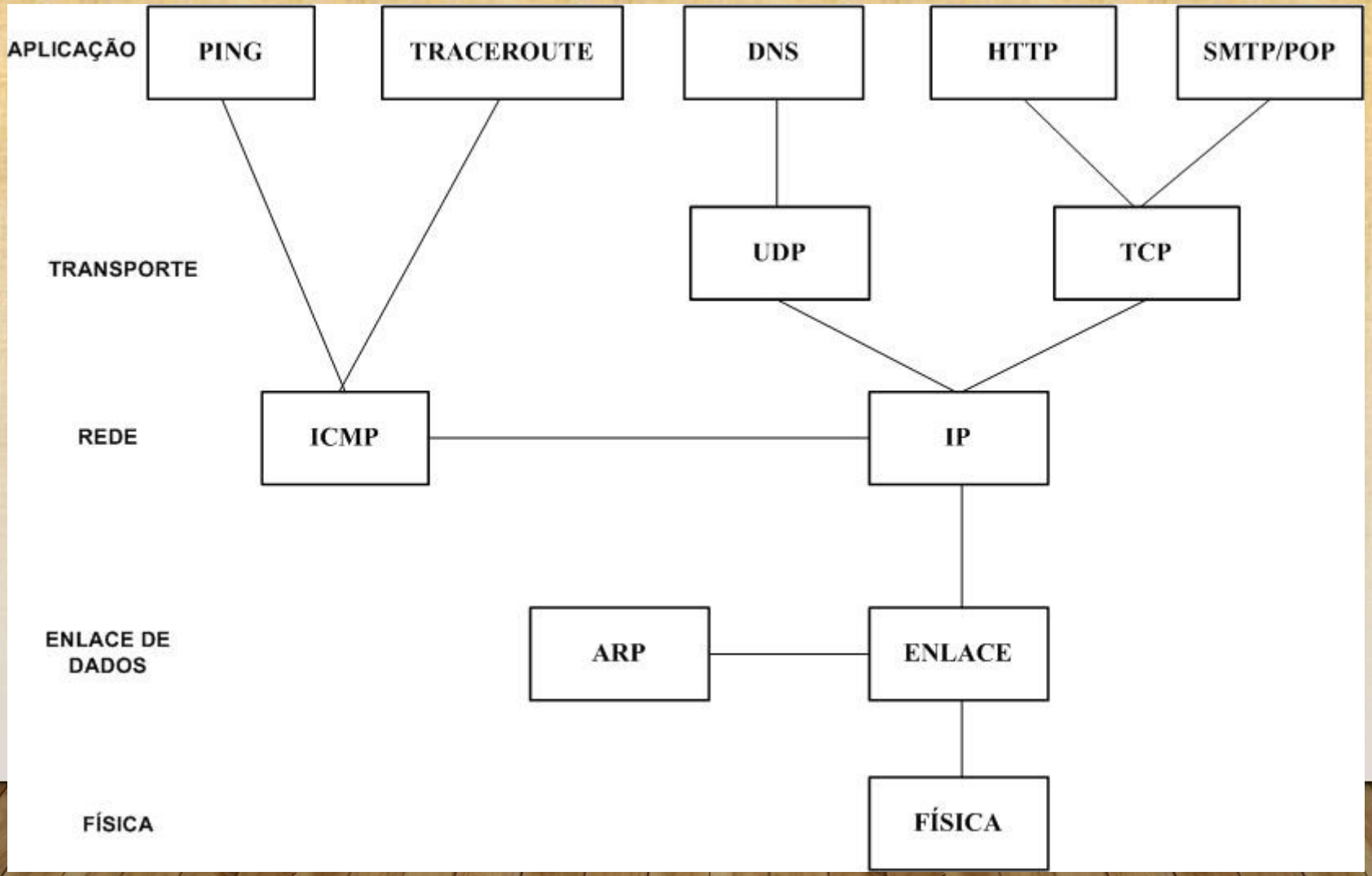
- O processo descrito anteriormente, por ser baseado em mensagens de broadcast, pode ter um impacto no desempenho da rede. Para evitar isso, as máquinas que originam a requisição ARP guardam o resultado numa tabela em memória chamada cache ARP.
- Cada computador em uma rede mantém sua própria tabela ARP. Sempre que um dispositivo de rede desejar enviar dados através de uma rede, usará informações fornecidas pela sua tabela ARP. Antes de realizar o processo descrito o cache é consultado, para evitar mensagens de broadcast desnecessárias;
- Esse dados são dinâmicos sendo armazenados por um período de tempo.

PROTOCOLO ARP

- Exemplo do ARP no sistema operacional *Linux*:
  - [root@localhost root]# arp

Address	HWtype	HWaddress
172.16.0.2	ether	00:04:75:EF:84:E8
172.16.0.10	ether	00:04:75:BC:A3:45

PROTOCOLOS (CAMADA DE REDE)

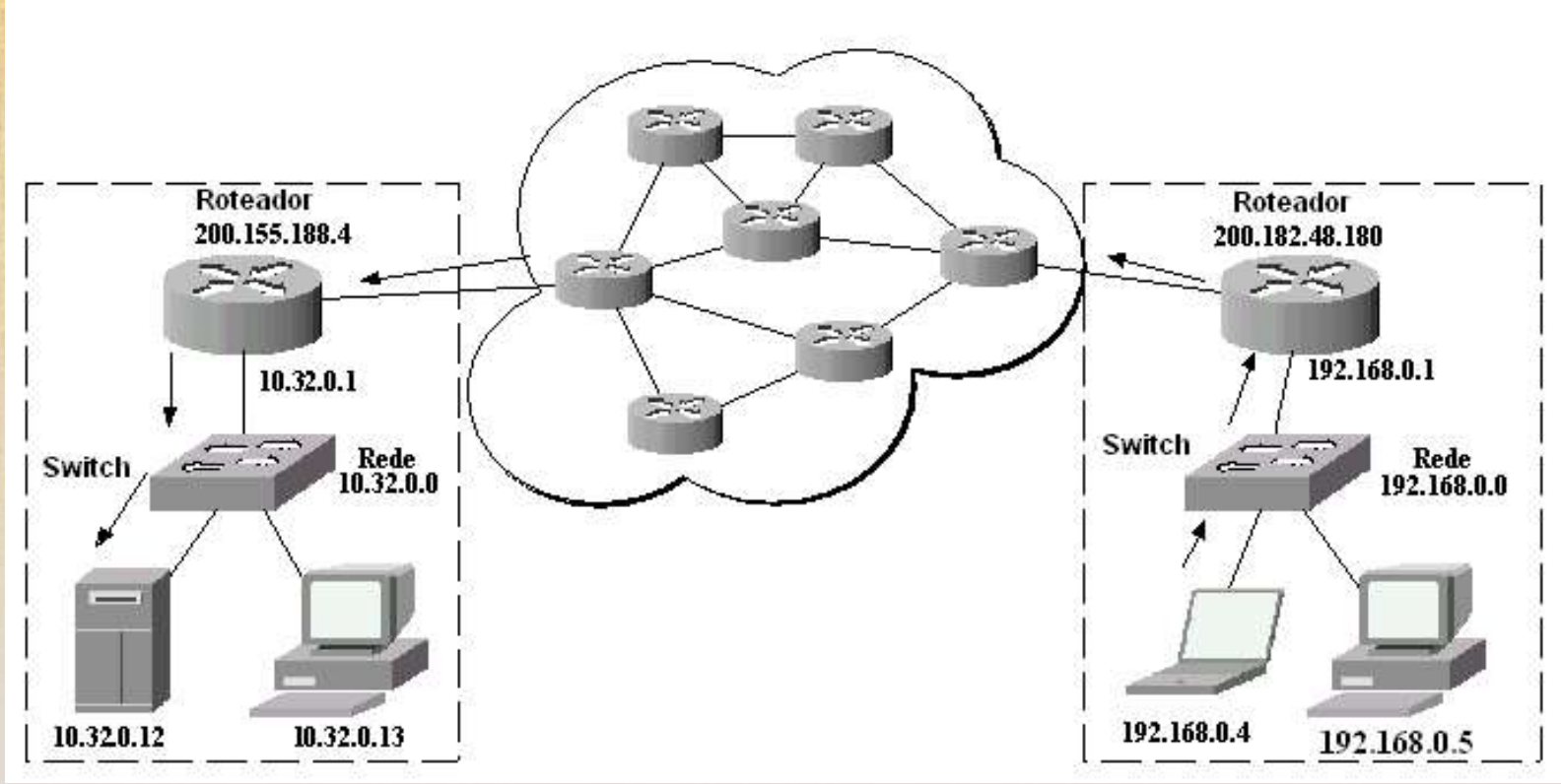


CAMADAS DE REDE - CARACTERÍSTICAS

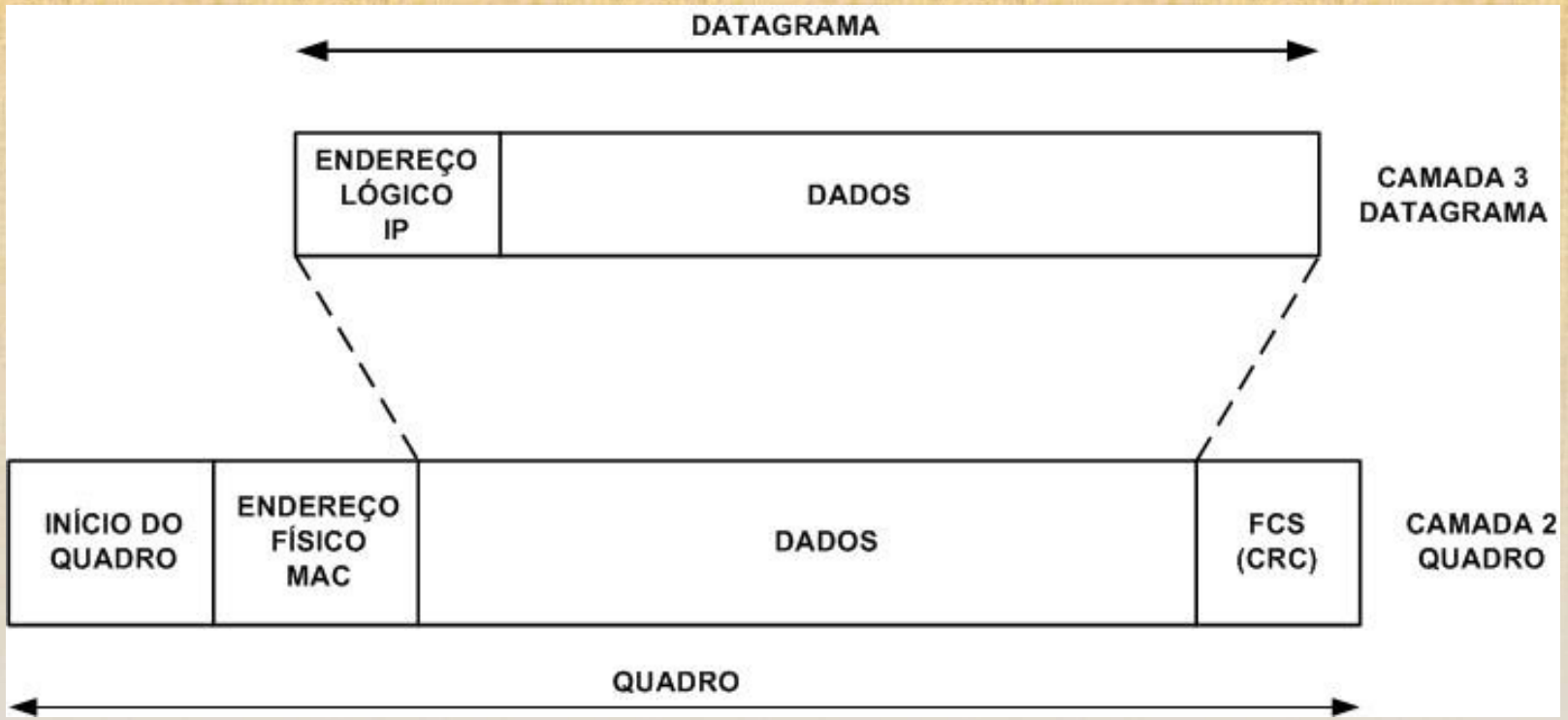
- Procotolo IP
  - Endereçamento estático (Manual) e dinâmico (DHCP);
- Formato do datagrama (IPV4, IPV6);
  - Protocolo ICMP
  - Mensagens de erros (Ping);
  - Sinalização de rotas (Traceroute);
- Roteamento
  - Estático;
  - Dinâmico (RIP, OSPF, etc);
  - Seleção de caminho;
  - Tabela de roteamento.

DETERMINAÇÃO DO CAMINHO

Qual o melhor caminho ?

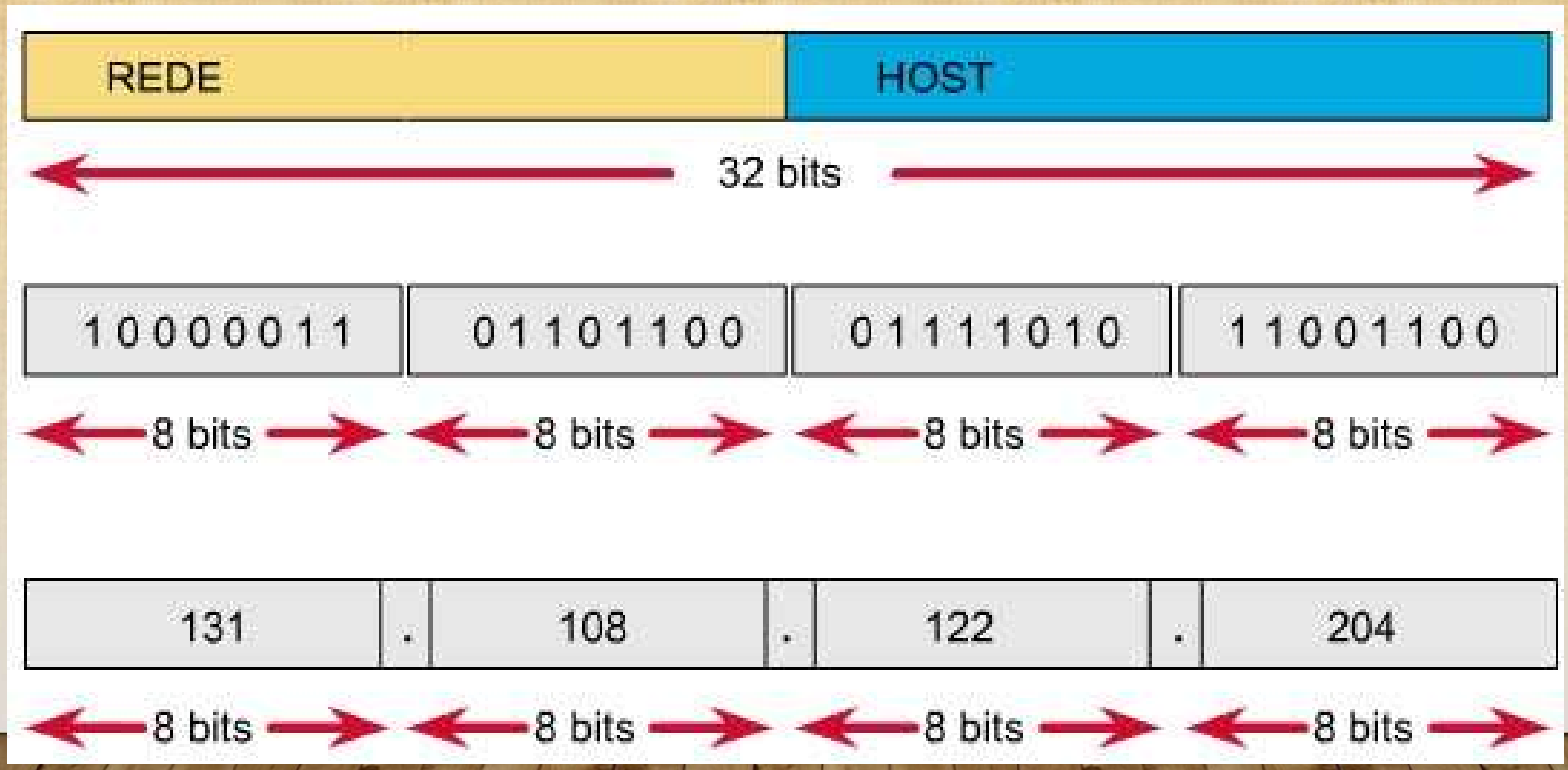


DATAGRAMAS

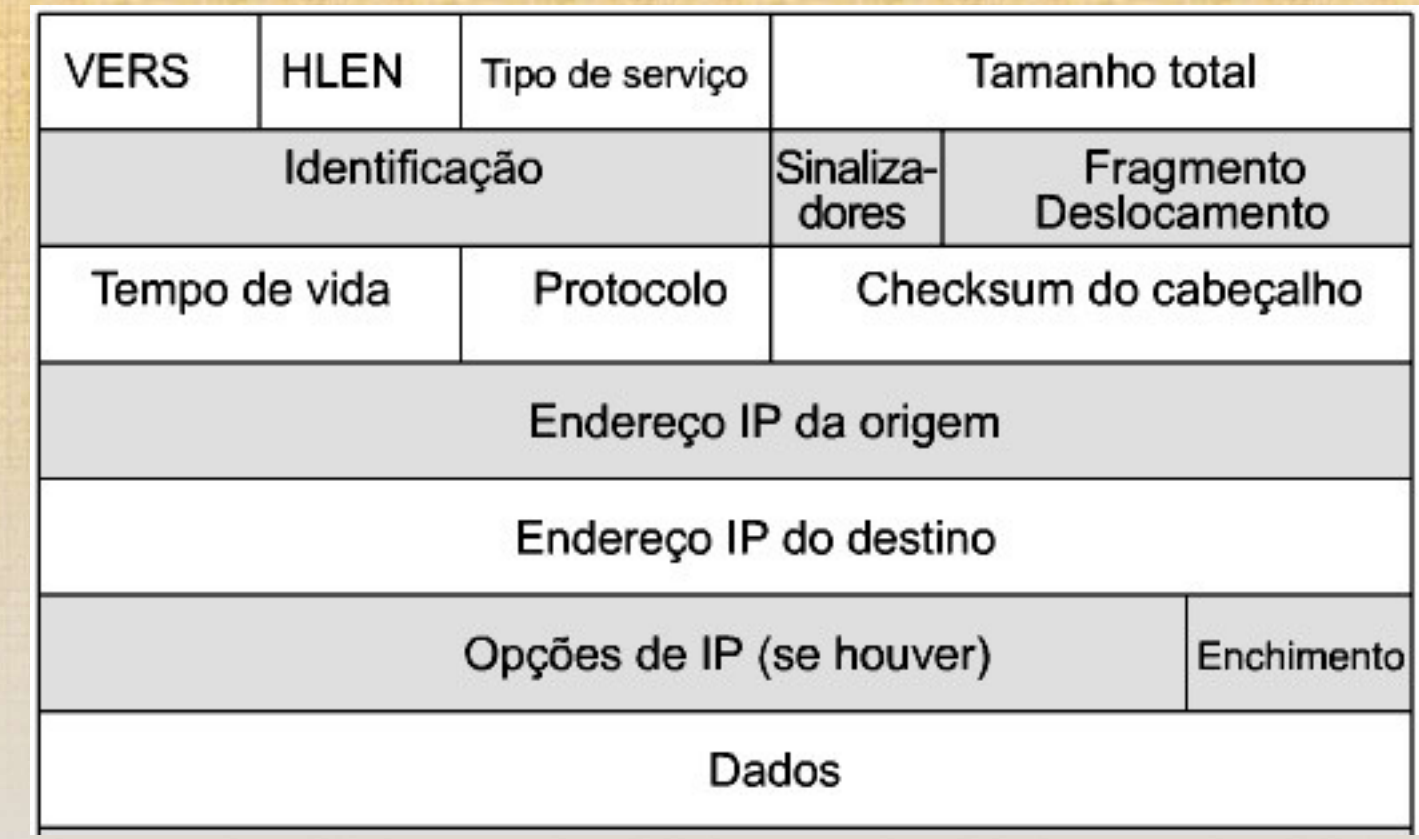

DATAGRAMA
ENDEREÇO LÓGICO IP
DADOS
CAMADA 3 DATAGRAMA
INÍCIO DO QUADRO
ENDEREÇO FÍSICO MAC
DADOS
FCS (CRC)
CAMADA 2 QUADRO
QUADRO

DATAGRAMAS

- Representação do endereço IP



FORMATO DE UM DATAGRAMA



CAMPOS DO DATAGRAMA IP

- Os pacotes/datagramas da camada 3 tornam-se dados da camada 2, que são encapsulados em quadros. Analogamente, o pacote IP consiste em dados de camadas superiores mais um cabeçalho IP, que consiste em:
  - versão - indica a versão de IP usada atualmente e o formato do cabeçalho (IPV4);
  - tamanho do cabeçalho IP (HLEN) - indica o tamanho do cabeçalho do datagrama em palavras de 32 bits;

CAMPOS DO DATAGRAMA IP

- tipo de serviço - especifica o nível de importância que foi atribuído por um determinado protocolo de camada superior (8 bits);
- tamanho total - especifica o tamanho total do pacote IP, incluindo dados e cabeçalho, em bytes (pode conter até 65.536 Bytes, porém esse número é impraticável, o tamanho máximo é de 576 Bytes – 64 Bytes de cabeçalho + 512 Bytes de dados);
- identificação (ID)- contém um número inteiro que identifica o datagrama atual (auxilia na reconstrução de datagramas fragmentados);
- sinalizadores (flags) – identifica os datagramas fragmentados (1=mais fragmentos, 0=último);

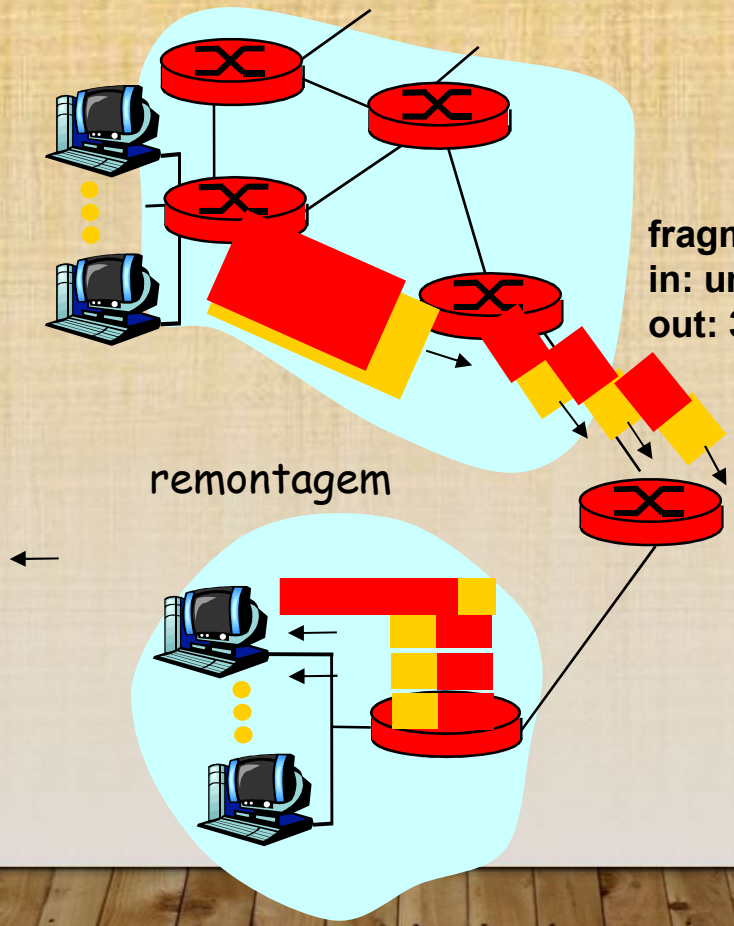
CAMPOS DO DATAGRAMA IP

- deslocamento de fragmento (fragment offset) - o campo que é usado para ajudar a juntar fragmentos de datagramas (indica o ponto em que o datagrama pertence a uma mensagem fragmentada);
- time-to-live (TTL) - mantém um contador que diminui gradualmente, por incrementos, até zero, momento em que o datagrama é descartado, evitando que os pacotes permaneçam infinitamente em loop (8 bits);
- protocolo – contém o protocolo usado na camada superior (TCP,UDP);
- checksum do cabeçalho - ajuda a assegurar a integridade do cabeçalho IP (16 bits);

CAMPOS DO DATAGRAMA IP

- endereço de origem - especifica o nó origem (32 bits);
- endereço de destino - especifica o nó destino (32 bits);
- opções - permite que o IP suporte várias opções (registro de rota, listagem de roteadores, etc);
- dados - contêm informações de camada superior (TCP ou UDP + dados);
- enchimento - zeros adicionais são adicionados a esse campo para assegurar que o cabeçalho IP seja sempre um múltiplo de 32 bits.

FRAGMENTAÇÃO E REMONTAGEM IP



fragmentação
in: um datagrama grande
out: 3 datagramas menores

FRAGMENTAÇÃO E REMONTAGEM IP

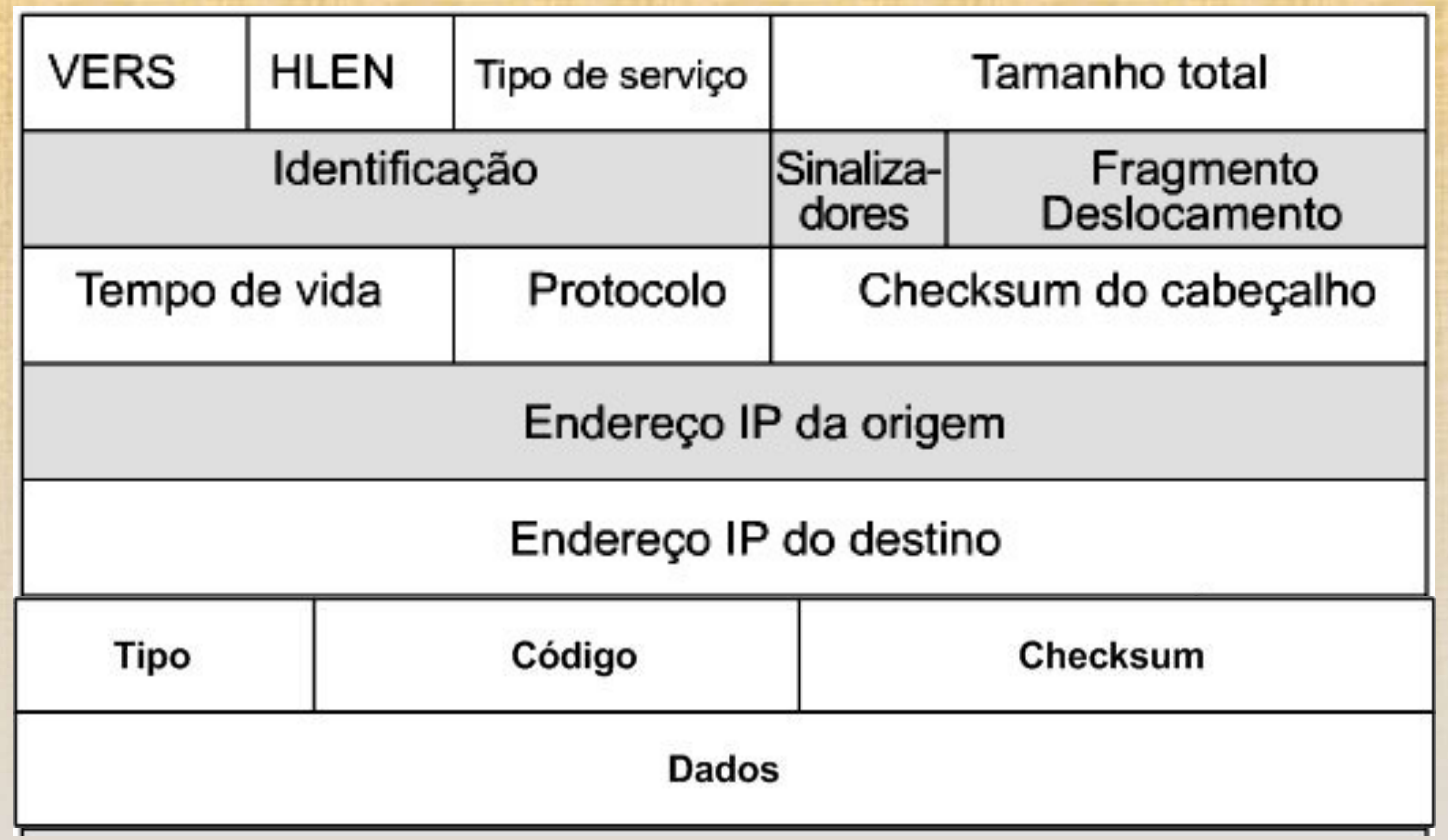
- enlaces de rede têm MTU (max. transfer size) - corresponde ao maior quadro que pode ser transportado pela camada de enlace.
  - tipos de enlaces diferentes possuem MTU diferentes (ethernet: máx de 1518 bytes)
- datagramas IP grandes devem ser divididos dentro da rede (fragmentados)
  - um datagrama dá origem a vários datagramas
  - “remontagem” ocorre apenas no destino final
  - O cabeçalho IP é usado para identificar e ordenar datagramas relacionados

FRAGMENTAÇÃO E REMONTAGEM IP

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

- Indica erros na rede, congestionamento na rede, número de pulos excedidos, etc.
- usado por computadores e roteadores para troca de informação de controle da camada de rede
  - error reporting: host, rede, porta ou protocolo
  - echo request/reply (usado pela aplicação ping)
- transporte de mensagens:
  - mensagens ICMP transportadas em datagramas IP
- ICMP message: tipo, código, mais primeiros 8 bytes do datagrama IP que causou o erro

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)



ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Tipo	Código	descrição
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 (Time Exceeded)
15	0	Information Request
16	0	Information Reply

ICMP (PING)

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

ICMP (PING)

- O utilitário Ping é utilizado para testar a conexão com outro computador. O Ping utiliza o protocolo ICMP para enviar uma mensagem ao computador remoto e aguarda uma resposta contendo a mesma mensagem (*echo*).
- O Ping deve reportar o tempo de ida e volta da mensagem (RTT– Round Trip Time), o tamanho da mensagem de dados (padrão de 32 bytes) e o tempo de vida (TTL). No final do teste, é gerada uma estatística, mostrando todas as informações coletadas no teste.

ICMP (TRACEROUTE)

- Tracert

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

ICMP (TRACEROUTE)

- Visualroute

Hop	IP Address	Node Name	Location
0	200.189.84.177	cnet-cable-189-84-177.canbrasnet.com.br	*
1	200.189.84.1	cnet-cable-189-84-1.canbrasnet.com.br	(Brazil)
2			
3	200.189.80.1	router.canbrasnet.com.br	(Brazil)
4	200.228.240.29	embratel-A4-0-63-gacc04.spo.embratel.net.br	Sao Paulo, Brazil
5	200.230.243.16	-	(Brazil)
6	200.246.244.6	intelig-P7-0-gacc05.spo.embratel.net.br	Sao Paulo, Brazil
7			
8			
9	200.201.131.3	-	(Brazil)
10	200.170.211.110	200-170-211-110.core01.spo.ifx.net.br	(Brazil)
11			
12	**200.155.188.4**	www.maua.br	(Brazil)

Roundtrip time to www.maua.br, average = 113ms, min = 51ms, max = 207ms -- 22/Fev/05 8:49 (Collapse Table)

ICMP (TRACEROUTE)

- NeotracePro