Protocolo ICMP

Alfredo Gama de Carvalho Júnior
Empresa Brasileira de Telecomunicações S.A.

Gerência de Operações RN/PB/AL/SE
agama@embratel.com.br

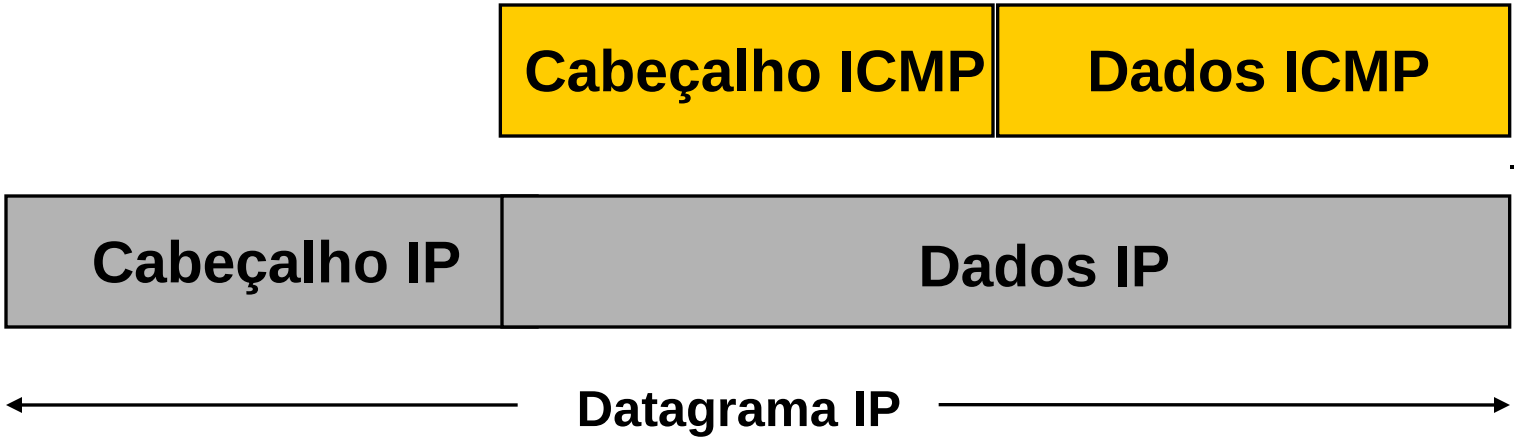
Natal - Novembro 2001

Protocolo ICMP

- Auxilia o protocolo IP gerando mensagens de erro que indicam possíveis falhas na entrega (best effort delivery)
- Funções:
  - Sinalizar erros: ttl exceed, destination unreachable
  - Trocar informações:
  - Diagnosticar conectividade: ping, traceroute
- Depende dos Protocolos das camadas superiores para garantir a confiabilidade.
- Relata a origem falhas na entrega de pacotes sem corrigi-las.

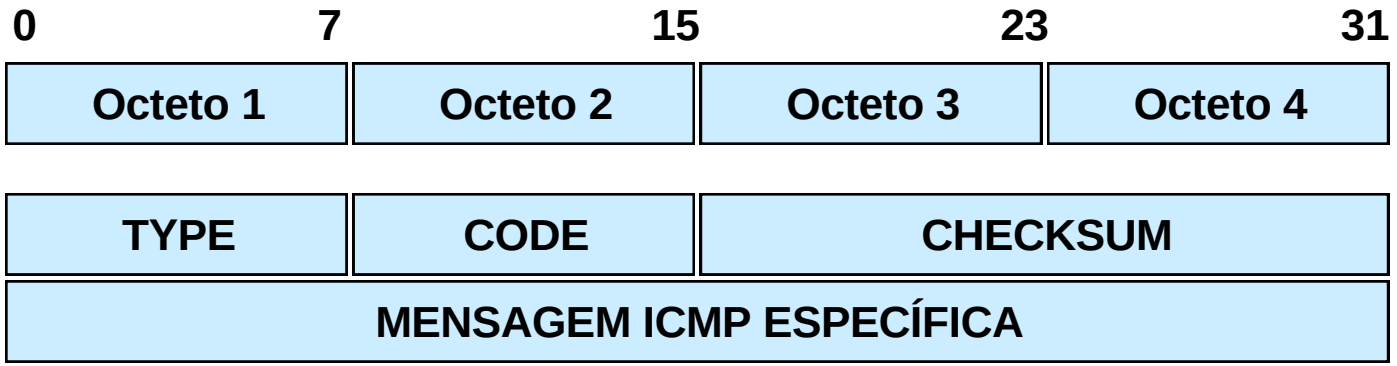
Protocolo ICMP

- Encapsulada no protocolo IP (PROTO=1) e roteada normalmente como uma mensagem IP .



Protocolo ICMP

- Um identificador principal de tipo (TYPE) e um identificador de sub-tipo (CODE)
- TYPE- Categoriza as mensagens ICMP
- CODE - Informação adicional conforme TYPE
- CHECKSUM - Considera header e dados



Protocolo ICMP

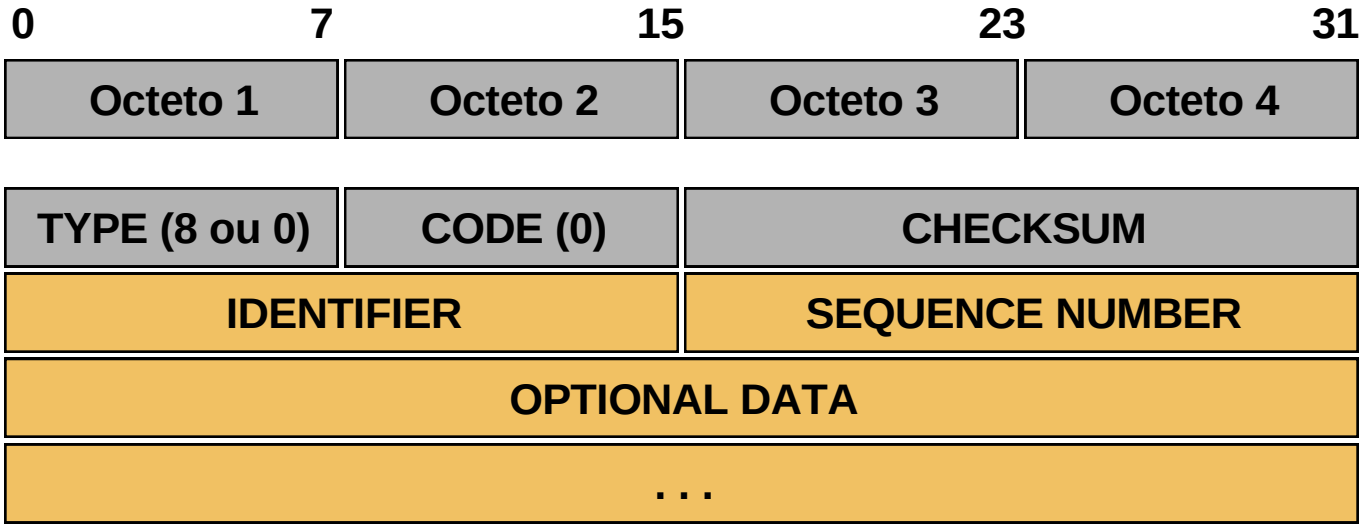
- A mensagem ICMP é geralmente destinada ao host origem da mensagem, não existindo nenhum mecanismo para informar erros aos roteadores no caminho ou ao host destino.

Tipo	Mensagem ICMP	Categoria
0	Echo Reply	Controle
3	Destination Unreachable	Erro
4	Source Quench	Controle
5	Redirect	Controle
8	Echo Request	Controle
9	Router Advertisement (RFC 1256)	Controle
10	Router Solicitation (RFC 1256)	Controle
11	Time Exceeded for a Datagram	Erro
12	Parameter Problem on a Datagram	Erro
13	Timestamp Request	Controle
14	Timestamp Reply	Controle
15	Information Request (obsoleto)	Controle
16	Information Reply (obsoleto)	Controle
17	Address Mark Request	Controle
18	Address Mark Reply	Controle

Protocolo ICMP

- Mensagens ICMP não são geradas para indicar erros devido mensagens ICMP, Broadcast ou Multicast.
- Evita saturação de link e queda de LANs face Broadcast Storms
- As mensagens ICMP que sinalizam erros carregam em seu campo DATA, além de informações relativas ao erro sinalizado, o header e os primeiros 8 bytes de dados do datagrama que as motivou.

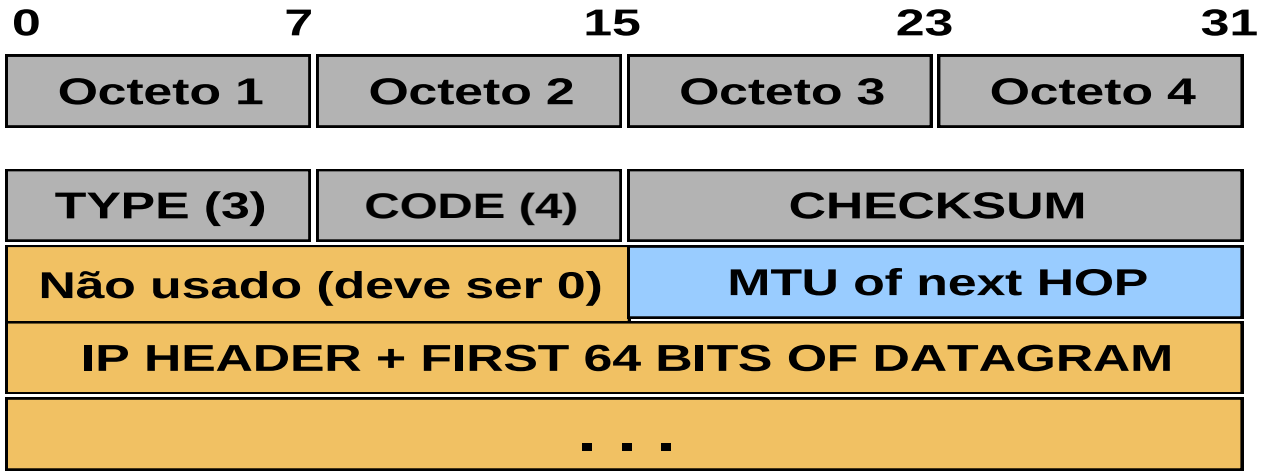
Echo Request e Echo Reply



- Utilizada pelo comando ping
- É utilizada principalmente para fins de testes de conectividade (endereçamento e roteamento) entre as duas máquinas.

Destination Unreacheable

- Notifica impossibilidade de entrega do datagrama
- Código identifica motivo da impossibilidade de alcançar o destino



Destination Unreacheable

0 - Network Unreachable - Rede destino inacessível

1 - Host Unreachable (ou falha no roteamento para subnet) - Máquina destino inacessível

2 - Protocol Unreachable - Protocolo destino desativado ou aplicação inexistente

3 - Port Unreachable - Porta destino sem aplicação associada

Destination Unreacheable

4 - Fragmentation Needed and DNF set -

Fragmentação necessária mas bit DNF setado.

Utilizado como forma de um host descobrir o menor MTU nas redes que serão percorridas entre a origem e o destino (ICMP MTU Discovery Protocol).

5 - Source Route Failed - Roteamento por rota especificada em opção IP, falhou

Destination Unreacheable

6 - Destination Network Unknown

7 - Destination Host Unknown

8 - Source Host Isolated

9 - Communication with destination network administratively prohibited

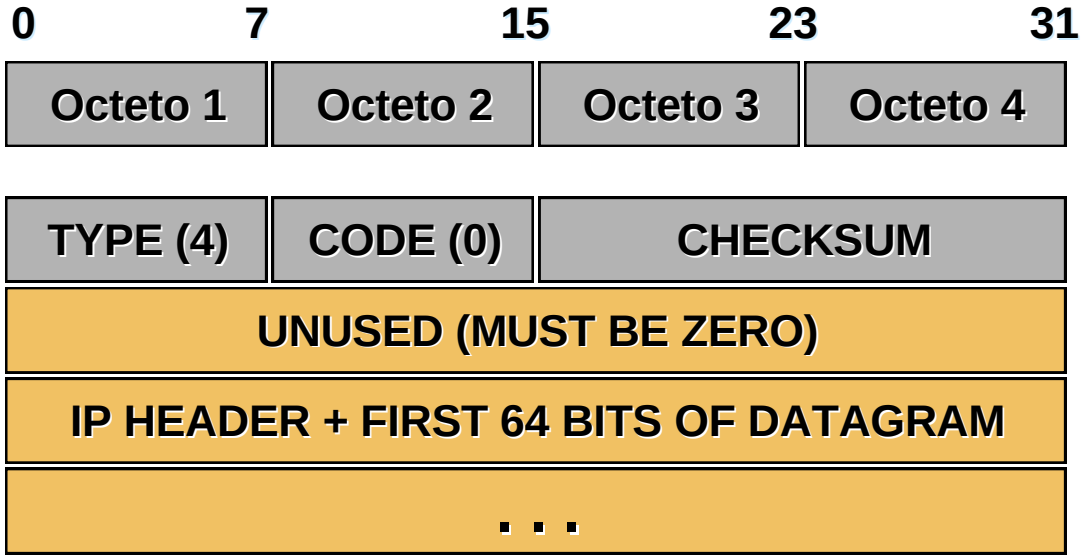
10 - Communication with destination host administratively prohibited

11 - Network unreacheable for type of service

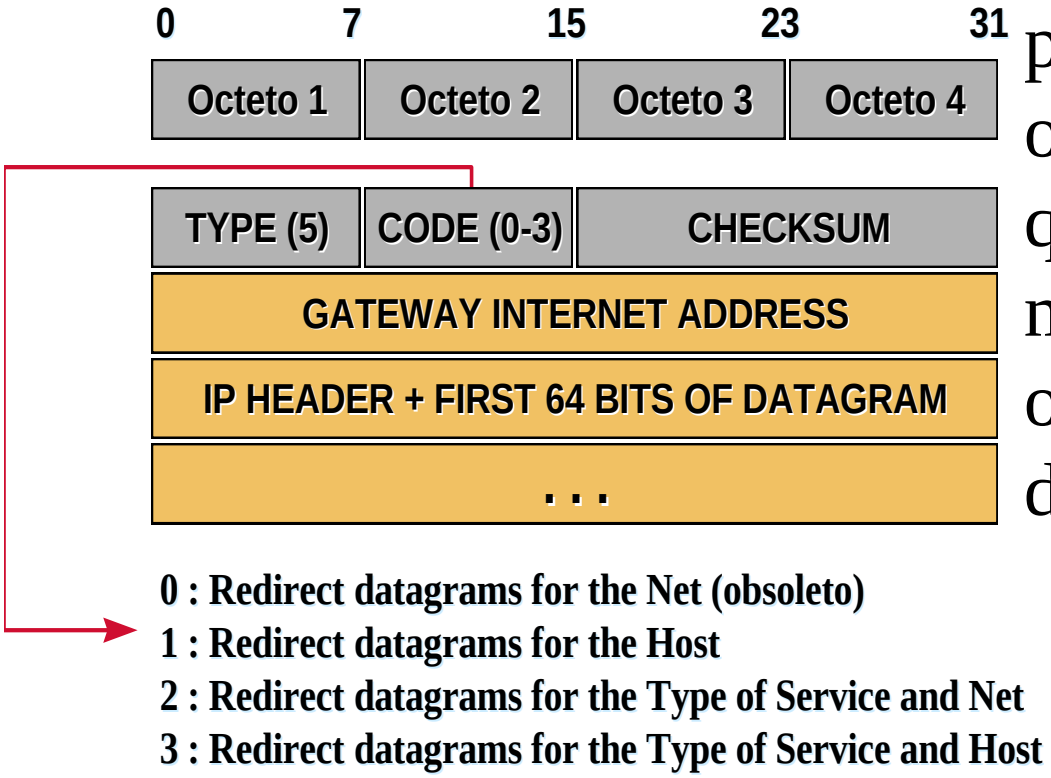
12 - Host unreacheable for type of service

Source Quench

- **Utilizada por um roteador para informar ao host origem, o descarte do pacote devido a incapacidade de roteá-lo por causa do tráfego.**
- **Hosts geradores de pacotes reduzem a taxa de envio.**



Redirect

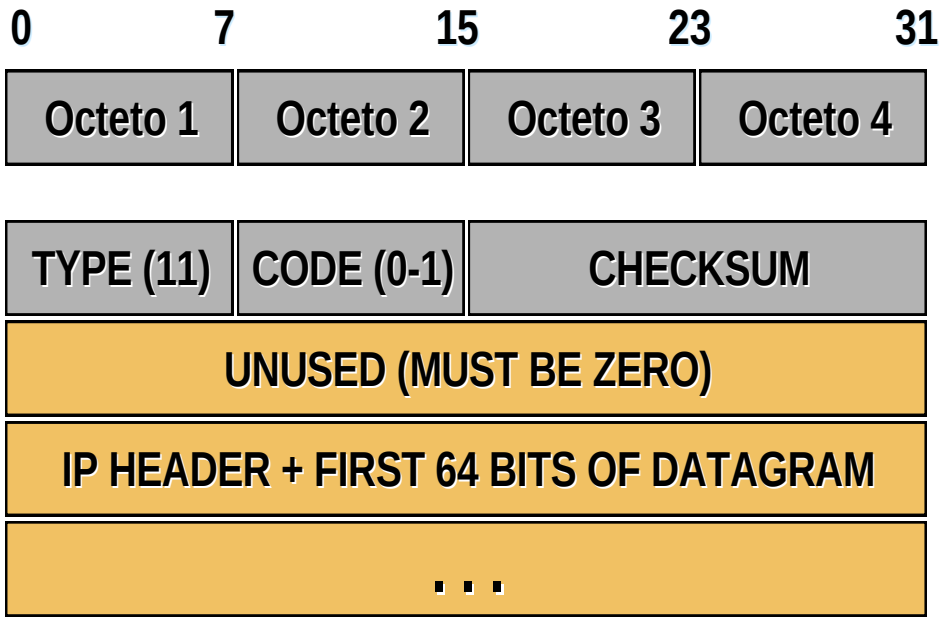


Utilizada por roteadores para informar ao host origem de uma mensagem que existe uma rota direta mais adequada através de outro roteador, para envio dos próximos datagramas.

Redirect

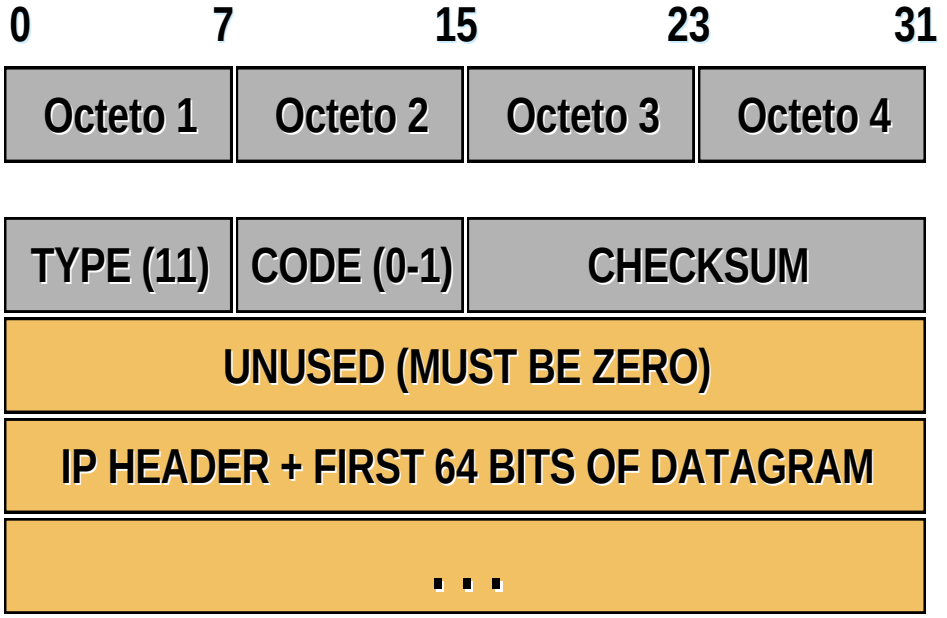
- CODE:
  - 0: Redirect datagrams for the Net
  - 1: Redirect datagrams for the Host
  - 2: Redirect datagrams for the Type of Service and Net
  - 3: Redirect datagrams for the Type of Service and Host
  - * Obsoleto

TTL Expired



- Mensagem ICMP originada em um roteador que informa ao host de origem que foi obrigado a descartar o pacote, uma vez que o TTL chegou a zero, ou pelo Host destino para informar término do tempo para REMONTAGEM.
- Traceroute

TTL Expired



- Code (0) :
  - **Temporizador do Tempo de Vida.**
- Code (1) :
  - **Tempo de Remontagem de Fragmentos Excedido.**

ICMP Router Solicitation/Advertisement

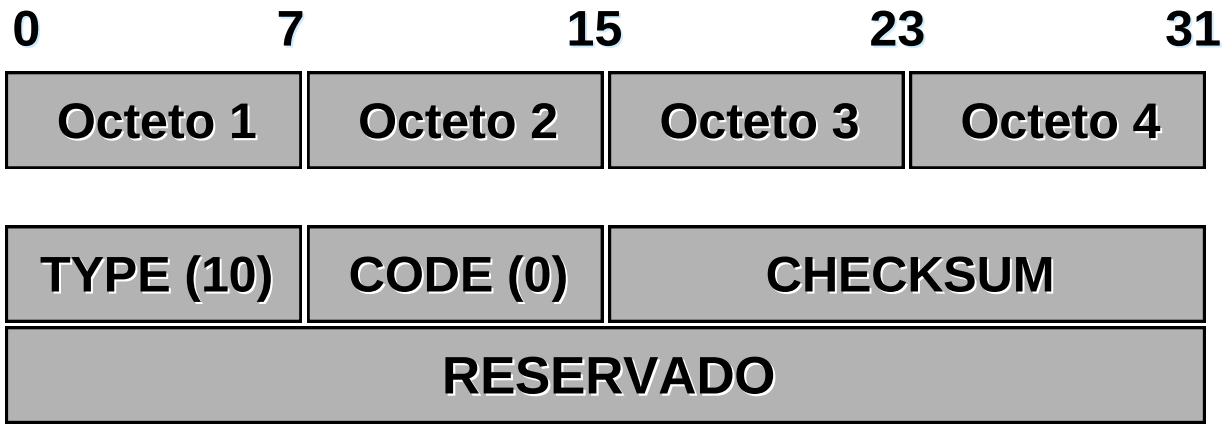
- Foi projetada para permitir que um roteador possa divulgar sua existência para as máquinas presentes na rede.
- Objetivo:
  - **Evitar a configuração manual das estações da rede com a rota default**
  - **Permitir que uma estação conheça outros roteadores além do default (roteamento no caso de falha do principal).**

ICMP Router Solicitation/Advertisement

- A mensagem é composta de duas formas:
  - **a solicitação de divulgação de um roteador**
  - **o anúncio de um roteador.**
- Configuração do roteador:
  - **envio automático das mensagens de anúncio**
  - **comandado por uma mensagem de solicitação.**

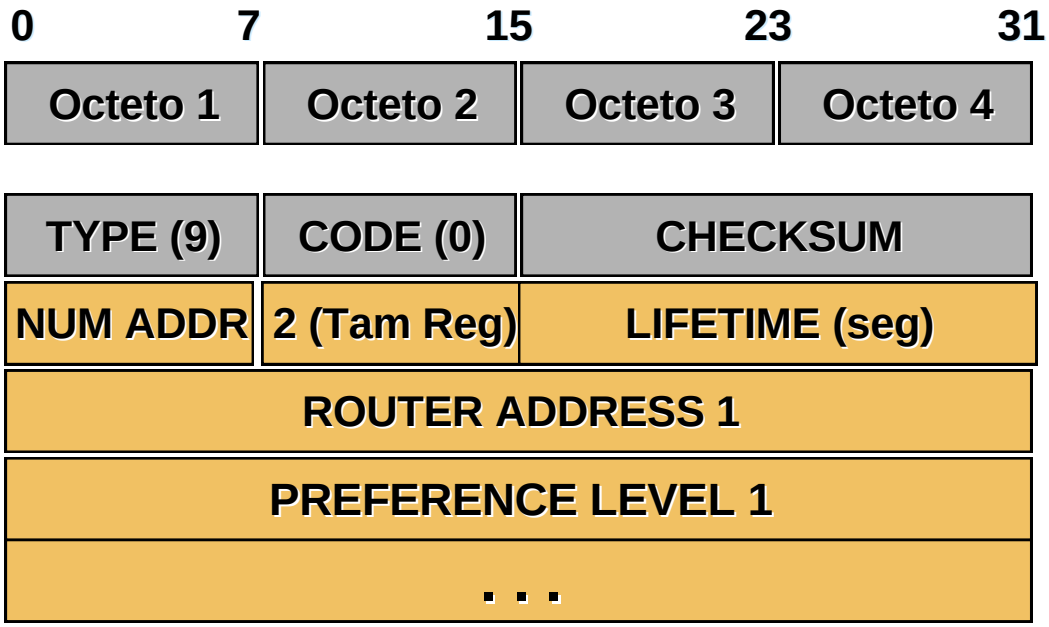
ICMP Router Solicitation

- A mensagem ICMP Router Solicitation é mostrada abaixo :



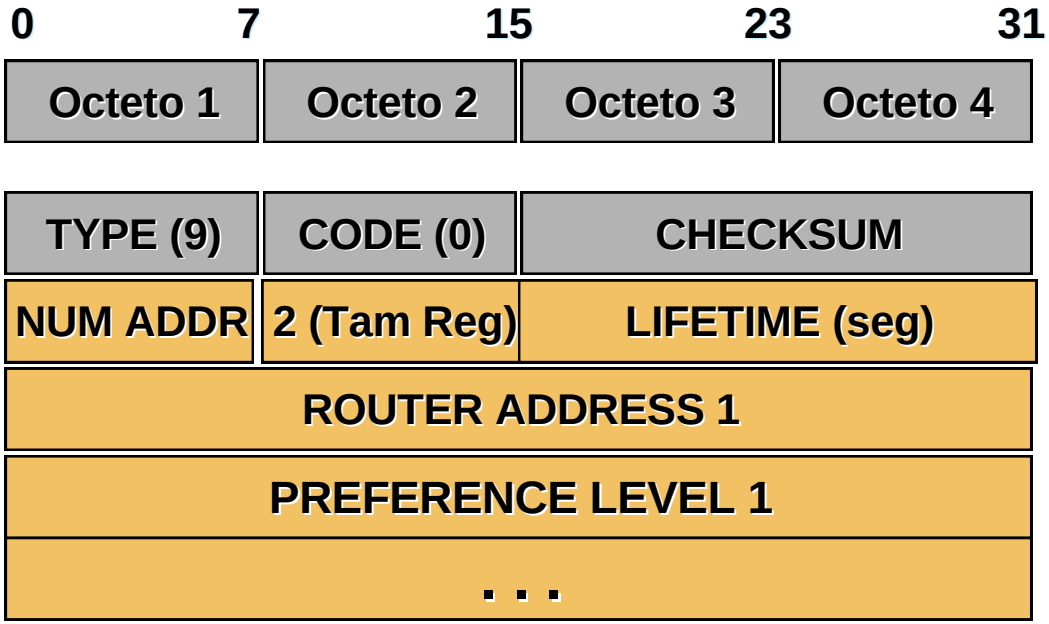
ICMP Router Advertisement

- Contém a divulgação de diversos roteadores iniciada a partir de um que seja configurado para divulgá-los.



ICMP Router Advertisement

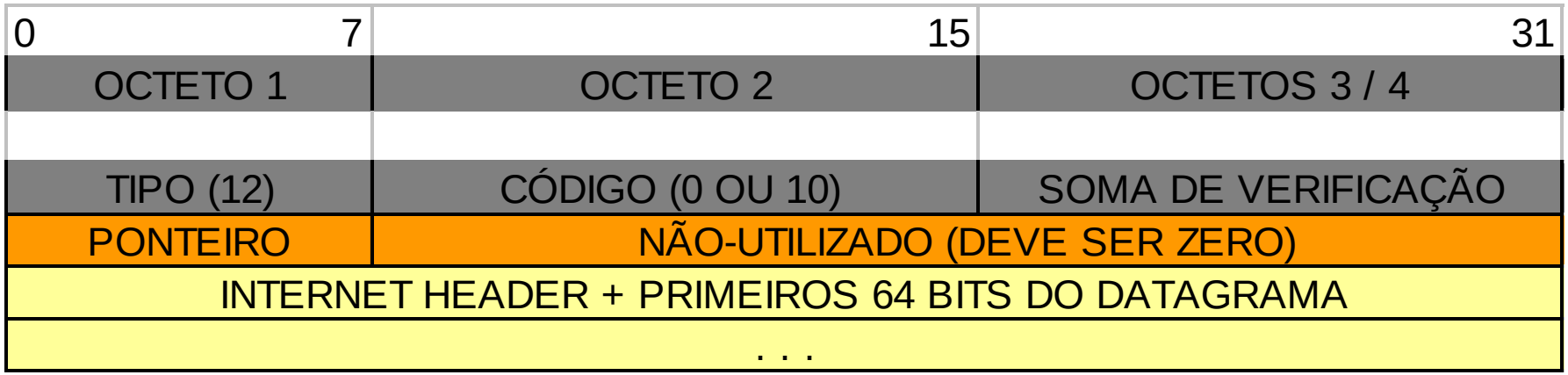
- O número de preferência é a ordem de preferência que estes roteadores podem ser utilizados pelas estações.



Parameter Problem Datagram

- Quando um Router ou um host encontra problema com o datagrama que não esteja coberto pelas mensagens de erro ICMP, ele envia uma mensagem de **problema de parâmetro** ao transmissor.

Parameter Problem Datagram



Utilização de um campo PONTEIRO para identificar o octeto do datagrama que originou o problema.

Timestamp Request/Reply

- Cada máquina mantém sua própria noção de tempo presente (operação independente).
- Problema: diferenças entre relógios podem confundir usuários em sistemas distribuídos.
- Os hosts utilizam os 3 campos de indicação de horas para:
  - **Calcular as estimativas do tempo decorrido entre elas**
  - **Sincronizar os relógios**

Timestamp Request/Reply

0 7	15	31
OCTETO 1	OCTETO 2	OCTETOS 3 / 4
TIPO (13 OU 14)	CÓDIGO (0)	SOMA DE VERIFICAÇÃO
IDENTIFICADOR		NÚMERO DE SEQÜÊNCIA
ORIGINAR TIMBRE DE HORA		
RECEBER TIMBRE DE HORA		
TRANSMITIR TIMBRE DE HORA		

ORIGINAR TIMBRE DE HORA

Preenchido antes da transmissão pelo originador.

RECEBER TIMBRE DE HORA

Preenchido após o recebimento da solicitação.

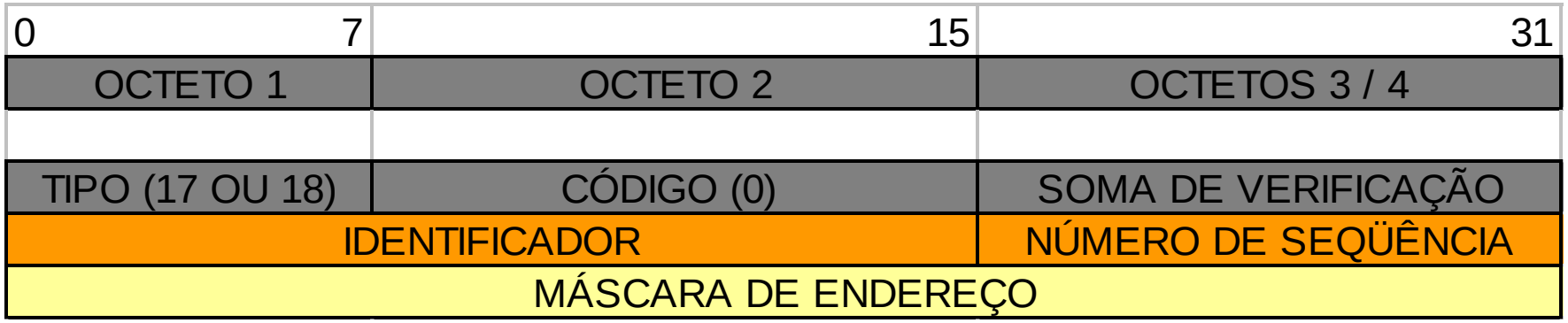
TRANSMITIR TIMBRE DE HORA

Preenchido antes do envio da resposta.

Address Mark Request/Reply

- Para conhecer a máscara de sub-rede utilizada pela rede central, a máquina pode enviar uma mensagem de **solicitação de máscara de endereço** a um roteador e receber uma **resposta de máscara de endereço.**
- A transmissão da solicitação pode ser:
  - Direta: se souber o endereço do roteador.
  - Broadcast: se não souber.

Address Mask Request/Reply



Information Request/Reply

- Permite que os hosts descubram seus endereços na interligação em redes quando da inicialização do sistema.
- Considerado obsoleto hoje em dia.
- Substituído pelo BOOTP , RARP e DHCP

Comando PING

- Testa a conexão entre dois computadoress ou a configuração TCP/IP no computador local (loopback)
- Envia um ***echo request*** e espera por um ***echo reply***. Por segurança, envia vários ***echo request*** .
- Testa o tempo de ida e volta de um pacote. Isso possibilita verificar se a rede está lenta, porém, não pode ser utilizado como ferramenta para avaliar o desempenho da rede.

Comando PING - Sintaxe

```
C:\WINDOWS.000>ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] destination-list

Opções:
    -t             Fazer ping para o host especificado até parada.
                   Para ver estatísticas e continuar - digite 'Control-Break';
                   Para parar - digite 'Control-C'.
    -a             Resolver endereços para nomes de hosts.
    -n count       Número de pedidos de eco para envio.
    -l size        Enviar tamanho do buffer.
    -f             Definir sinalizador 'Não fragmentar' no pacote.
    -i TTL         Time To Live.
    -v TOS         Tipo de serviço.
    -r count       Registrar rotas para saltos de contagem.
    -s count       Marca de hora para saltos de contagem.
    -j host-list   Rota ampliada de origens usada com host-list.
    -k host-list   Rota restrita para host-list.
    -w timeout     Marca de hora em milissegundos para aguardar cada resposta.
```

PING - Resultados

- Sem resposta
  - Indica não haver conexão
- Perda de pacotes (significante quando > 2-3%)
  - Devido a erros de transmissão, sobrecarga nas WANs/LANs ou nos switches/routers
- Tempo de resposta variando
  - sobrecarga de host/network
  - >100 ms inaceitável para trabalho interativo (telnet)
- Sem perda e tempo constante

PING - Exemplos

Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS.000>ping www.embratel.net.br

Disparando contra www.embratel.net.br [200.255.125.213] com 32 bytes de dados:

Resposta de 200.255.125.213:bytes=32 tempo=494ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=535ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=520ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=505ms Tempo de vida=238

Estatísticas do Ping para 200.255.125.213:
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
Mínimo = 494ms, Máximo = 535ms, Média = 513ms

PING - Exemplos

C:\WINDOWS.000>ping 200.255.125.213

Disparando contra 200.255.125.213 com 32 bytes de dados:

Resposta de 200.255.125.213:bytes=32 tempo=503ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=545ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=530ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=515ms Tempo de vida=238

Estatísticas do Ping para 200.255.125.213:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
    Mínimo = 503ms, Máximo = 545ms, Média = 523ms

C:\WINDOWS.000>

PING - Exemplos

Microsoft(R) Windows 98
(C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS.000>ping -n 1 www.embratel.net.br

Disparando contra www.embratel.net.br [200.255.125.213] com 32 bytes de dados:

Resposta de 200.255.125.213:bytes=32 tempo=526ms Tempo de vida=238

Estatísticas do Ping para 200.255.125.213:
Pacotes: Enviados = 1, Recebidos = 1, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
Mínimo = 526ms, Máximo = 526ms, Média = 526ms

C:\WINDOWS.000>

PING - Exemplos

C:\WINDOWS.000>ping -l 64 200.255.125.213

Disparando contra 200.255.125.213 com 64 bytes de dados:

Resposta de 200.255.125.213:bytes=64 tempo=1038ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=64 tempo=1154ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=64 tempo=495ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=64 tempo=535ms Tempo de vida=238

Estatísticas do Ping para 200.255.125.213:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
    Mínimo = 495ms, Máximo = 1154ms, Média = 805ms

C:\WINDOWS.000>

PING - Exemplos

C:\WINDOWS.000>ping -f 200.255.125.213

Disparando contra 200.255.125.213 com 32 bytes de dados:

Resposta de 200.255.125.213:bytes=32 tempo=530ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=570ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=560ms Tempo de vida=238
Resposta de 200.255.125.213:bytes=32 tempo=550ms Tempo de vida=238

Estatísticas do Ping para 200.255.125.213:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
    Mínimo = 530ms, Máximo = 570ms, Média = 552ms

C:\WINDOWS.000>

TRACERT - TRACEROUTE

- Traça a rota entre dois computadores, isto é, retorna os endereços IP dos roteadores intermediários entre o equipamento local e remoto
- Como?
  - Envia mensagem UDP para uma **unused port** na máquina destino **com ttl=1**
  - Roteador decrementa ttl para 0 e retorna mensagem ICMP de **time exceed**
  - traceroute seta **ttl =2 and retransmite**, a mensagem atinge o próximo **hop**
  - **ttl** é incrementado até que a mensagem UDP alcançar o destino.
  - A máquina destino retorna uma mensagem ICMP **service unavailable** porque a solicitação foi para uma porta “inexistente”

TRACERT - Sintaxe

```
C:\WINDOWS.000>tracert

Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite]
destino

Opções:
    -d                Não resolver endereços para nomes de hosts.
    -h nmax_saltos     Número máximo de saltos para a procura do
destino.
    -j lst_hosts       Rota ampliada de origens usada com a lista lst_hosts.
    -w tempo_limite    Tempo de espera em milissegundos para cada
resposta.

C:\WINDOWS.000>
```

Normalmente envia 3 mensagens para cada Roteador

A mensagem que não retorna é marcada com *

TRACERT - Exemplos

C:\WINDOWS.000>tracert -d 200.255.125.213

Rastreando a rota para 200.255.125.213 com no máximo 30 saltos

1	363 ms	362 ms	385 ms	64.12.104.235
2	375 ms	385 ms	385 ms	64.12.104.252
3	370 ms	385 ms	330 ms	64.12.130.61
4	370 ms	440 ms	330 ms	204.148.102.189
5	370 ms	935 ms	330 ms	204.148.97.205
6	375 ms	385 ms	385 ms	204.148.98.69
7	375 ms	385 ms	440 ms	204.148.97.89
8	430 ms	440 ms	440 ms	204.148.99.98
9	430 ms	330 ms	330 ms	204.148.99.178
10	430 ms	330 ms	440 ms	208.178.174.53
11	430 ms	440 ms	440 ms	206.132.253.198
12	595 ms	495 ms	550 ms	64.211.60.234
13	540 ms	550 ms	550 ms	200.255.197.14
14	540 ms	550 ms	550 ms	200.255.197.141
15	*	*	*	Esgotado o tempo limite do pedido.
16	505 ms	550 ms	550 ms	200.255.125.213

Rastreamento completo.

TRACERT - Exemplos

```
C:\WINDOWS.000>tracert 200.255.125.213

Rastreando a rota para wks13.rjo.embratel.net.br [200.255.125.213]
com no máximo 30 saltos:

  1   329 ms   330 ms   330 ms  ipt-me06.proxy.aol.com [64.12.104.235]
  2   370 ms   440 ms   330 ms  tot8-mc3-G3-1.proxy.aol.com [64.12.104.252]
  3   920 ms   330 ms   330 ms  wc2-mc3-P4-1.aol.com [64.12.130.61]
  4   425 ms   440 ms   439 ms  pop2-mtc-P3-0.atdn.net [204.148.102.189]
  5   427 ms  1427 ms   440 ms  204.148.97.205
  6   430 ms   330 ms   440 ms  204.148.98.69
  7   980 ms  1980 ms   440 ms  bb1-dcl-P4-0.atdn.net [204.148.97.89]
  8   375 ms   330 ms   330 ms  pop1-dcl-P5-1.atdn.net [204.148.99.98]
  9   370 ms   330 ms   385 ms  globalcenter.atdn.net [204.148.99.178]
 10  1470 ms   935 ms   935 ms  pos2-0-155M.cr1.WDC2.gblx.net [208.178.174.53]
 11   425 ms  1430 ms  1430 ms  pos0-0-622M.cr2.NYC3.gblx.net [206.132.253.198]

 12   549 ms   550 ms   550 ms  EmpresaakaEmbratel1.pos1-0.cr2.NYC3.gblx.net [64
.211.60.234]
 13   535 ms   550 ms   550 ms  ebt-P5-0-core03.rjo.embratel.net.br [200.255.197
.14]
 14   540 ms  2090 ms   495 ms  ebt-P6-0-dist04.rjo.embratel.net.br [200.255.197
.141]
 15     *        *        *     Esgotado o tempo limite do pedido.
 16   508 ms   546 ms   550 ms  wks13.rjo.embratel.net.br [200.255.125.213]

Rastreamento completo.
```

TRACERT - Exemplos

```
C:\WINDOWS.000>tracert -d -h 5 200.255.125.213

Rastreando a rota para 200.255.125.213 com no máximo 5 saltos

  1   976 ms   440 ms   329 ms  64.12.104.235
  2   370 ms   385 ms   330 ms  64.12.104.252
  3   375 ms   385 ms   385 ms  64.12.130.61
  4   430 ms   385 ms   385 ms  204.148.102.189
  5   370 ms   440 ms   440 ms  204.148.97.205

Rastreamento completo.

C:\WINDOWS.000>
```

TRACERT - Exemplos

```
C:\WINDOWS.000>tracert -d www.embratel.net.br

Rastreando a rota para www.embratel.net.br [200.255.125.213]
com no máximo 30 saltos:

  1   430 ms   330 ms   444 ms  64.12.104.235
  2   375 ms   935 ms   330 ms  64.12.104.252
  3   370 ms   385 ms   330 ms  64.12.130.61
  4   920 ms   385 ms   385 ms  204.148.102.189
  5   370 ms  1155 ms   385 ms  204.148.97.205
  6   370 ms   330 ms   385 ms  204.148.98.69
  7   375 ms   385 ms  2420 ms  204.148.97.89
  8   385 ms  1925 ms   330 ms  204.148.99.98
  9  1640 ms   385 ms   507 ms  204.148.99.178
 10   370 ms   440 ms     *     208.178.174.53
 11   350 ms   385 ms   440 ms  206.132.253.198
 12   540 ms   550 ms  1155 ms  64.211.60.234
 13   935 ms   550 ms   550 ms  200.255.197.14
 14   540 ms   550 ms   550 ms  200.255.197.141
 15     *        *        *     Esgotado o tempo limite do pedido.
 16   543 ms   605 ms   495 ms  200.255.125.213

Rastreamento completo.

C:\WINDOWS.000>
```