

ICMP (Internet Control Message Protocol)

Prof. Michel Sales Bonfim

Disciplina: Internet e Arquitetura TCP/IP

Introdução

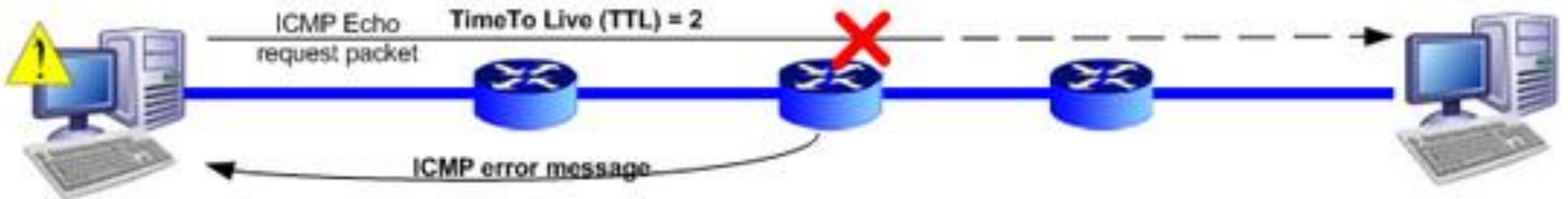
- ▶ O protocolo **IP** oferece um **serviço não confiável** (Sem conexão);
- ▶ Problemas para a entrega correta de datagramas:
 - ▶ Excesso de tráfego em determinada rota;
 - ▶ Defeitos em conexões físicas;
 - ▶ Delays com tempos elevados;
 - ▶ Tabelas de roteamento com problemas de integridade;
 - ▶ Destino inativo.
- ▶ **Não podemos contar com o protocolo IP para descobrir a origem destes eventuais problemas!**

Protocolo ICMP

- ▶ O ICMP é um protocolo de controle das transmissões pela rede;
- ▶ Definido na [RFC 792](#);
- ▶ Ele opera enviando **mensagens de erro** para o **transmissor** quando algum pacote encontra problema na transmissão;
 - ▶ Somente reporta, não corrige;
 - ▶ Possui definido mais de 13 tipos de mensagens.
- ▶ Permite testar a conectividade, ao nível do IP, entre equipamentos:
 - ▶ Contudo, ICMP não relata erros que ocorram em mensagens ICMP.

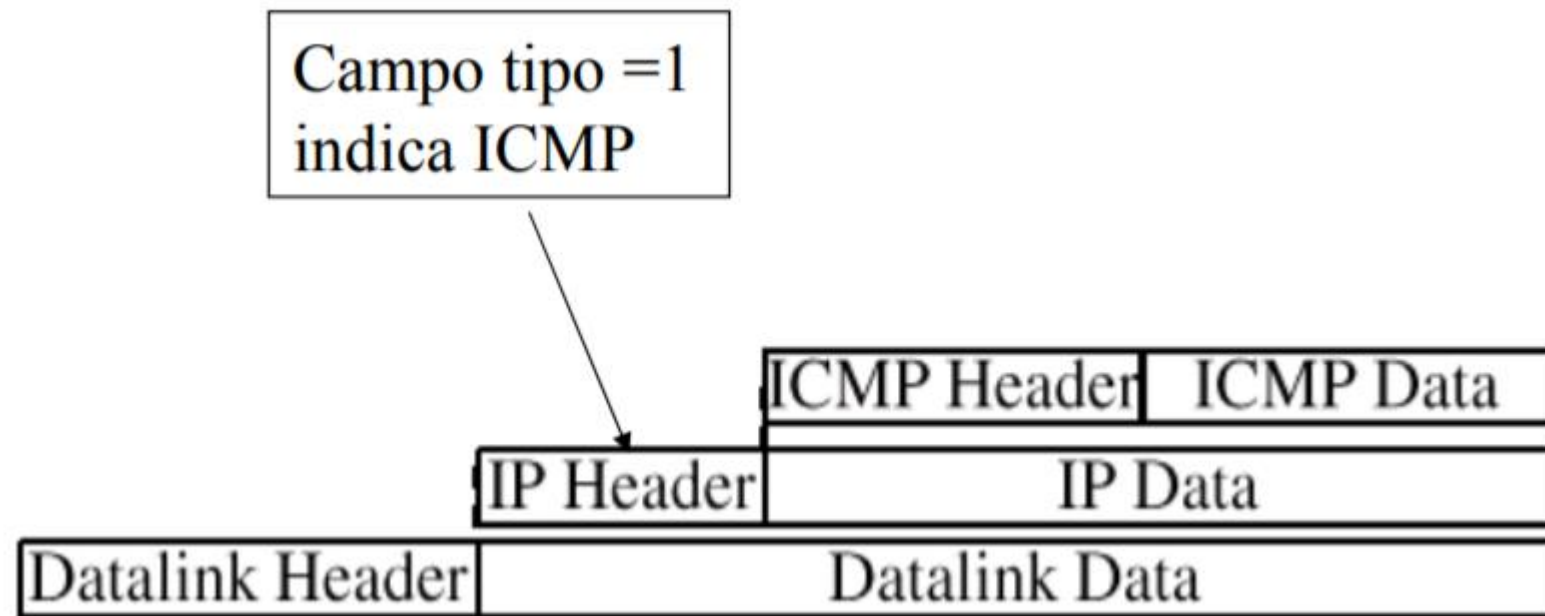
Protocolo ICMP

- ▶ Permite detectar falhas do tipo:
 - ▶ Falha nas linhas de comunicação;
 - ▶ Máquina destino desconectada da rede;
 - ▶ TTL (Time-to-Live) do pacote IP expirou;
 - ▶ Roteadores intermediários congestionados;
 - ▶ Etc.

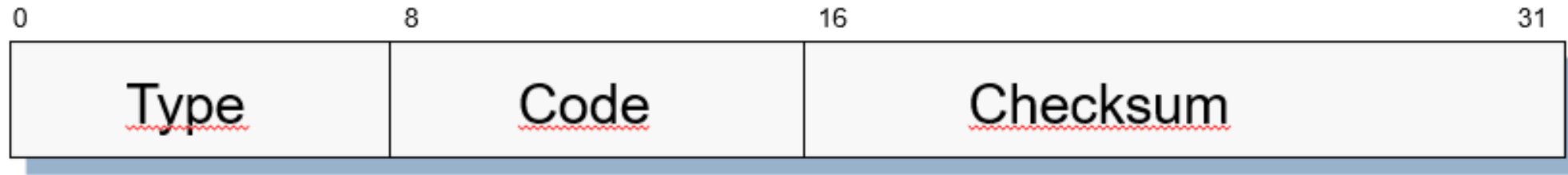


Protocolo ICMP

- ▶ Protocolo da Camada de Rede;
- ▶ Encapsulado em um datagrama IP.



Formato da Mensagem ICMP



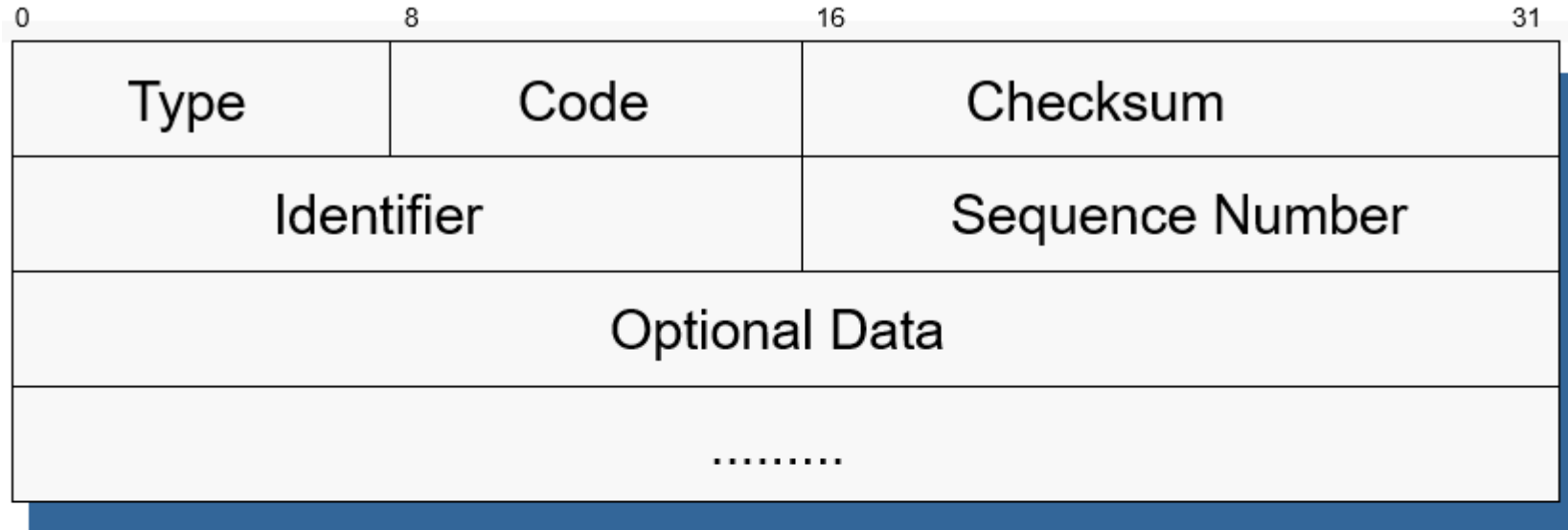
- ▶ Cada mensagem ICMP tem seu próprio formato, mas todas começam com os seguintes campos:
 - ▶ **TYPE (8 bits):** especifica o significado da mensagem e o formato do restante do pacote. Treze tipos foram definidos;
 - ▶ **CODE (8 bits):** contém o código de erro para o datagrama, reportado pela mensagem ICMP;
 - ▶ **CHECKSUM (16 bits):** é aplicado à toda mensagem, iniciando a partir do campo TYPE

Tipos de Mensagens ICMP

Tipo	Descrição
0	<u>Echo reply</u>
3	<u>Destination unreachable</u>
4	<u>Source quench</u>
5	<u>Redirect</u>
8	<u>Echo request</u>
11	<u>Time exceeded</u>
12	<u>Parameter unintelligible</u>
13	<u>Time-stamp request</u>
14	<u>Time-stamp reply</u>

Tipo	Descrição
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

Echo Request e Echo Reply



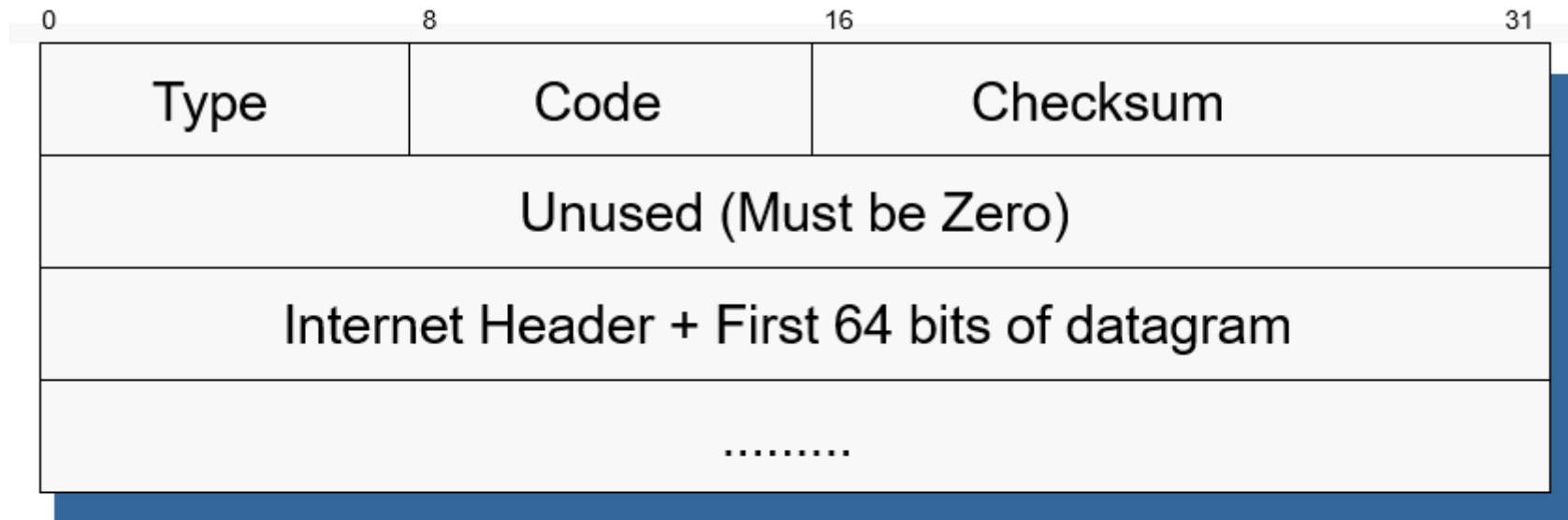
⇒ Type:

✓ 8 – Echo Request

✓ 0 – Echo Reply

⇒ Code: sempre zero (0)

Destination Unreachable



- ⇒ Type:
 - ✓ 3 - Destination Unreachable
- ⇒ Code:
 - ✓ Vários códigos específicos

Destination Unreachable

Código	Descrição
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation need and don't fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with dest net administratively prohibited
10	Communication with dest host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

Eventos mais comuns!

Tipo ICMP	Código	Descrição
0	0	resposta de eco (para <i>ping</i>)
3	0	rede de destino inalcançável
3	1	hospedeiro de destino inalcançável
3	2	protocolo de destino inalcançável
3	3	porta de destino inalcançável
3	6	rede de destino desconhecida
3	7	hospedeiro de destino desconhecido
4	0	repressão da origem (controle de congestionamento)
8	0	solicitação de eco
9	0	anúncio do roteador
10	0	descoberta do roteador
11	0	TTL expirado
12	0	cabeçalho IP inválido

Eventos mais comuns!

Tipo ICMP	Código	Descrição
0	0	resposta de eco (para <i>ping</i>)
3	0	rede de destino inalcançável
3	1	hospedeiro de destino inalcançável
3	2	protocolo de destino inalcançável
3	3	porta de destino inalcançável
3	6	rede de destino desconhecida
3	7	hospedeiro de destino desconhecido
4	0	repressão da origem (controle de congestionamento)
8	0	solicitação de eco
9	0	anúncio do roteador
10	0	descoberta do roteador
11	0	TTL expirado
12	0	cabeçalho IP inválido

Muitos provedores de Internet ativam filtros para o ICMP Tipo 8 (echo request) nos seus roteadores

Comando PING

Verificar se o Host destino esta ativo e qualificar a rota percorrida

```

Prompt de Comando

Microsoft Windows [versão 10.0.14393]
(c) 2016 Microsoft Corporation. Todos os direitos reservados.

C:\Users\JESUS>ping www.yahoo.com.br

Disparando src.g03.yahoodns.net [74.6.50.150] com 32 bytes de dados:
Resposta de 74.6.50.150: bytes=32 tempo=167ms TTL=53
Resposta de 74.6.50.150: bytes=32 tempo=168ms TTL=53
Resposta de 74.6.50.150: bytes=32 tempo=166ms TTL=53
Resposta de 74.6.50.150: bytes=32 tempo=167ms TTL=53

Estatísticas do Ping para 74.6.50.150:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
        perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 166ms, Máximo = 168ms, Média = 167ms

C:\Users\JESUS>ping www.naoexiste.com

Disparando www.naoexiste.com [92.242.140.6] com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.

Estatísticas do Ping para 92.242.140.6:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de
        perda),

```



RETORNO POSITIVO DO ICMP - ENCONTROU O HOST DESTINO



RETORNO NEGATIVO DO ICMP - NÃO ENCONTROU O HOST DESTINO

Comando PING

► Algumas opções importantes:

-t

Utilizando o -t, o comando ficará enviando pacotes até o usuário forçar a parada (com Ctrl + C).

-n (Windows) ou **-c** (Linux)

O comando define o número de pacotes a ser enviado.

Sintaxe: `ping -c 8 site.com.br`

(8 pacotes serão enviados pelo comando)

Comando TRACERT ou TRACEROUTE

Traçar a rota entre o Host origem e destino, detalhando o tempo utilizado

C:\> Prompt de Comando

```
Microsoft Windows [versão 10.0.14393]  
(c) 2016 Microsoft Corporation. Todos os direitos reservados.
```

```
C:\Users\JESUS>tracert www.yahoo.com.br
```

```
Rastreando a rota para src.g03.yahoodns.net [74.6.50.150]  
com no máximo 30 saltos:
```

1	1 ms	<1 ms	<1 ms	192.168.0.1
2	1 ms	1 ms	1 ms	192.168.1.1
3	8 ms	22 ms	22 ms	et-8-0-3-0.ptx-a.fac001.algartelem.com.br [201.48.84.105]
4	39 ms	39 ms	38 ms	et-12-0-1-0.ptx-a.spo-piaf.algartelem.com.br [170.84.35.5]
5	136 ms	135 ms	135 ms	ae0-0.border-b.mia.algartelem.com.br [170.84.34.9]
6	137 ms	153 ms	153 ms	ae3-0.border-a.ash.algartelem.com.br [170.84.34.18]
7	153 ms	153 ms	153 ms	exchange-cust1.dc2.equinix.net [206.126.236.16]
8	158 ms	159 ms	158 ms	ae-4-0.pat1.nyc.yahoo.com [216.115.104.121]
9	167 ms	167 ms	166 ms	ae-0.pat2.bfw.yahoo.com [216.115.111.30]
10	168 ms	168 ms	168 ms	et-18-1-0.msr1.bf2.yahoo.com [74.6.227.37]
11	169 ms	167 ms	166 ms	UNKNOWN-74-6-122-X.yahoo.com [74.6.122.59]
12	167 ms	167 ms	167 ms	po8.fab3-1-gdc.bf1.yahoo.com [72.30.22.37]
13	168 ms	167 ms	167 ms	po-11.bas1-10-prd.bf1.yahoo.com [69.147.72.133]
14	166 ms	166 ms	166 ms	w2.src.vip.bf1.yahoo.com [74.6.50.150]

Rastreamento concluído.