Laboratório 6.7.2: Examinando Pacotes ICMP

Diagrama de Topologia

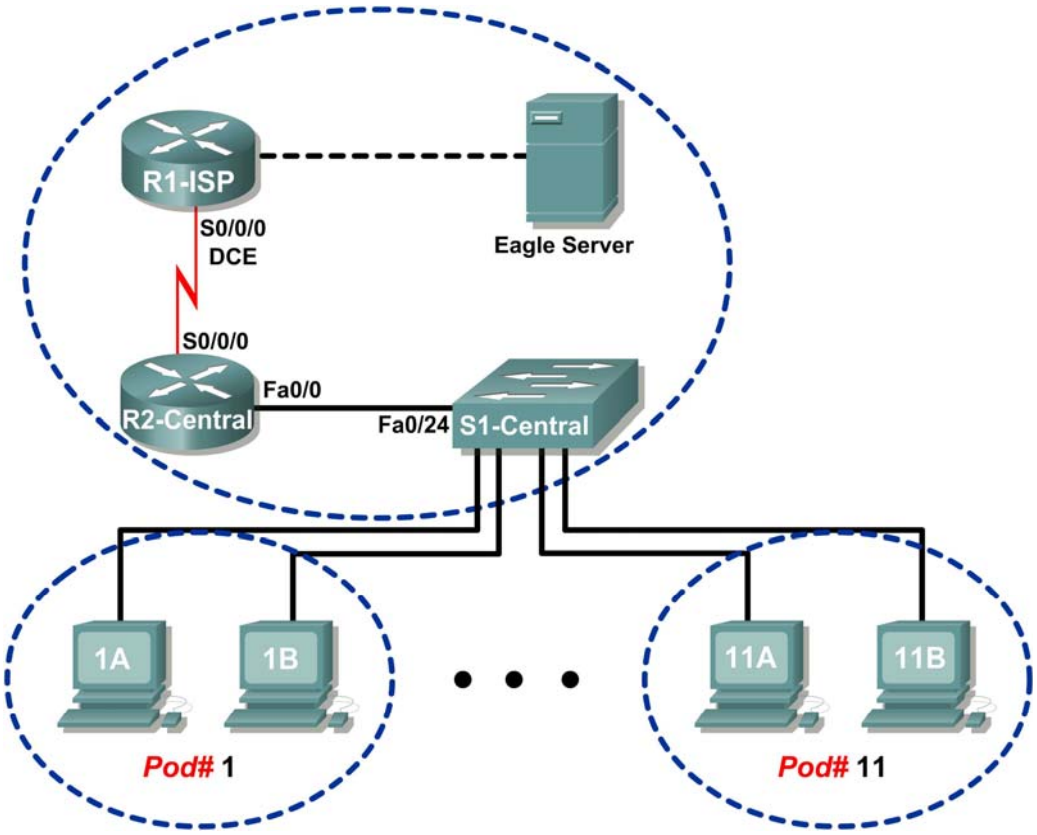


Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway Padrão
R1-ISP	**S0/0/0**	**10.10.10.6**	**255.255.255.252**	*N/A*
	Fa0/0	**192.168.254.253**	**255.255.255.0**	*N/A*
R2-Central	**S0/0/0**	**10.10.10.5**	**255.255.255.252**	*N/A*
	Fa0/0	**172.16.255.254**	**255.255.0.0**	*N/A*
Eagle Server	*N/A*	**192.168.254.254**	**255.255.255.0**	**192.168.254.253**
	N/A	**172.31.24.254**	**255.255.255.0**	*N/A*
host*Pod#***A**	*N/A*	**172.16.***Pod#***.1**	**255.255.0.0**	**172.16.255.254**
host*Pod#***B**	*N/A*	**172.16.***Pod#***.2**	**255.255.0.0**	**172.16.255.254**
S1-Central	*N/A*	**172.16.254.1**	**255.255.0.0**	**172.16.255.254**

Objetivos

Com a conclusão deste laboratório, você será capaz de:

- Entender o formato de pacotes ICMP.
- Usar o Wireshark para capturar e examinar mensagens ICMP.

Contexto

O Internet Control Message Protocol (ICMP) foi primeiramente definido no RFC 792, setembro de 1981. Os tipos de mensagem ICMP foram posteriormente expandidos no RFC 1700. O ICMP opera na camada de Rede TCP/IP e é usado para trocar informações entre dispositivos.

Os pacotes ICMP têm muitas utilizações nas redes de computador atuais. Quando um roteador não consegue entregar um pacote a uma rede ou a um host de destino, uma mensagem informacional é devolvida à origem. Além disso, os comandos **`ping`** e **`tracert`** enviam mensagens ICMP aos destinos e os destinos respondem com mensagens ICMP.

Cenário

Usando o Laboratório Eagle 1, serão feitas capturas Wireshark de pacotes ICMP entre dispositivos de rede.

Tarefa 1: Entendendo o Formato de Pacotes ICMP

Pacote ICMP – Informação de Cabeçalho de Mensagem Comum

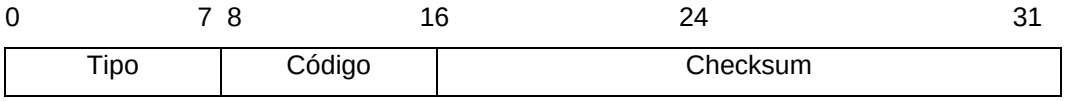


Figura 1. Cabeçalho de Mensagem ICMP

Consulte a Figura 1, os campos de cabeçalho ICMP comuns a todos os tipos de mensagem ICMP. Cada mensagem ICMP inicia com um campo de Tipo de 8-bits, um campo de Código de 8-bits e um Checksum de 16-bits. O tipo de mensagem ICMP descreve os campos ICMP restantes. A tabela na Figura 2 mostra tipos de mensagem ICMP do RFC 792:

Valor	Significado
0	Resposta de Echo
3	Destino Inalcançável
4	Source Quench
5	Redirect
8	Echo
11	Tempo Excedido
12	Problema de Parâmetro
13	Timestamp
14	Resposta Timestamp
15	Solicitação de Informação
16	Resposta de Informação

Figura 2. Tipos de Mensagem ICMP

Os códigos fornecem informações adicionais ao campo Tipo. Por exemplo, se o campo Tipo é 3, destino inalcançável, informações adicionais sobre o problema são devolvidas no campo Código. A Tabela na

Figura 3 mostra códigos de mensagem para uma mensagem ICMP de Tipo 3, destino inalcançável, do RFC 1700:

Código Valor	Significado
0	Rede Inalcançável
1	Host Inalcançável
2	Protocolo Inalcançável
3	Porta Inalcançável
4	Fragmentação Necessária e Não Fragmentar configurados
5	Falha da Rota de Origem
6	Rede de Destino Desconhecida
7	Host de Destino Desconhecido
8	Host de Origem Isolado
9	Comunicação com Rede de Destino Administrativamente Proibida
10	Comunicação com o Host de Destino é Proibida Administrativamente
11	Rede de Destino Inalcançável para Tipo de Serviço
12	Host de Destino Inalcançável para Tipo de Serviço

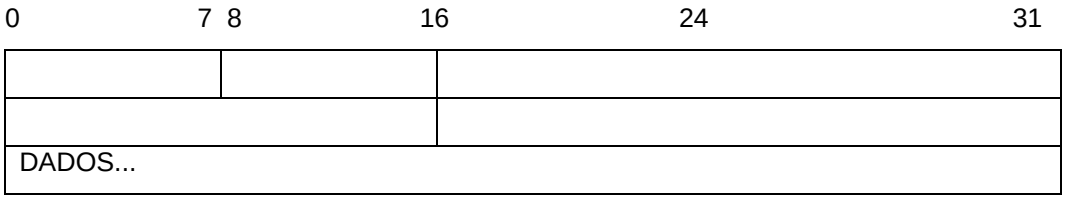
Figura 3. Códigos de Mensagem ICMP Tipo 3

Usando a captura de mensagem ICMP a na Figura 4, preencha os campos para a solicitação echo de pacote ICMP. Valores iniciados com `0x` são número hexadecimais:

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x365c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figura 4. Solicitação Echo de Pacote ICMP

Pacote ICMP - echo



Usando a captura de mensagem ICMP a na Figura 5, preencha os campos para a resposta de echo de pacote ICMP:


```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x3e5c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figura 5. Resposta de Echo de Pacote ICMP

Pacote ICMP – resposta echo

0	7	8	16	24	31
DADOS...					

Na camada de Rede TCP/IP, a comunicação entre dispositivos não é garantida. No entanto, o ICMP não fornece verificações mínimas para que uma resposta se equipare à solicitação. A partir das informações fornecidas nas mensagens ICMP acima, como o remetente sabe que a resposta é para um echo específico?

_____

_____

Tarefa 2: Usando o Wireshark para Capturar e Examinar Mensagens ICMP

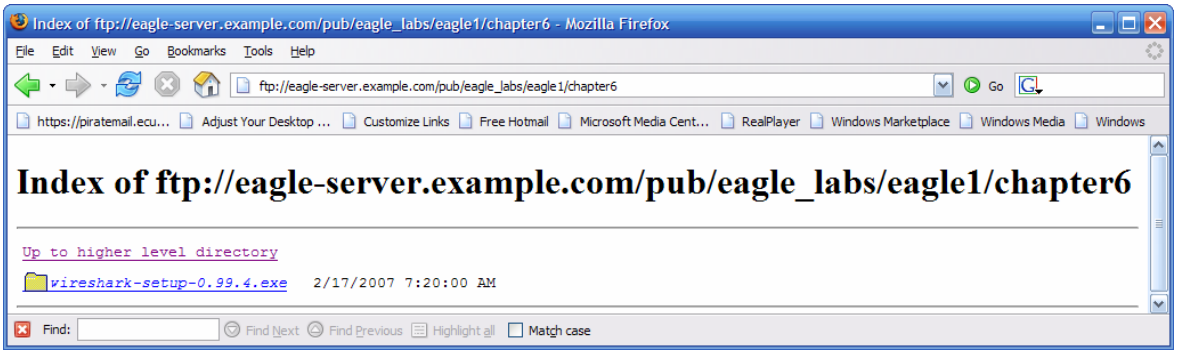


Figura 6. Site de Download do Wireshark

Se o Wireshark não estiver instalado no computador, você pode fazer o download do Eagle Server.

1. Abra um navegador, URL FTP://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6, como mostra a Figura 6.
2. Clique com o botão direito do mouse no nome de arquivo Wireshark, clique em **Salvar Link Como** e salve o arquivo no computador.
3. Quando o download do arquivo estiver concluído, abra e instale o Wireshark.

Passo 1: Capturar e avaliar mensagens de echo ICMP ao Eagle Server

Neste passo, o Wireshark será usado para examinar mensagens de echo ICMP.

1. Abra um terminal Windows no computador.
2. Quando estiver pronto, inicie a captura Wireshark.

```
C:\> ping eagle-server.example.com
Pinging eagle-server.example.com [192.168.254.254] with 32 bytes of
data:
Reply from 192.168.254.254: bytes=32 tempo<1ms TTL=63
Reply from 192.168.254.254: bytes=32 tempo<1ms TTL=63
Reply from 192.168.254.254: bytes=32 tempo<1ms TTL=63
Reply from 192.168.254.254: bytes=32 tempo<1ms TTL=63
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\ >
```

Figura 7. Respostas de `ping` com Sucesso do Eagle Server

3. Do terminal Windows, faça **`ping`** no Eagle Server. Quatro respostas com sucesso devem ser recebidas do Eagle Server, como mostra a Figura 7.
4. Pare a captura Wireshark. Deve haver um total de quatro solicitações de echo ICMP e respostas de echo combinadas, similares as da Figura 8.

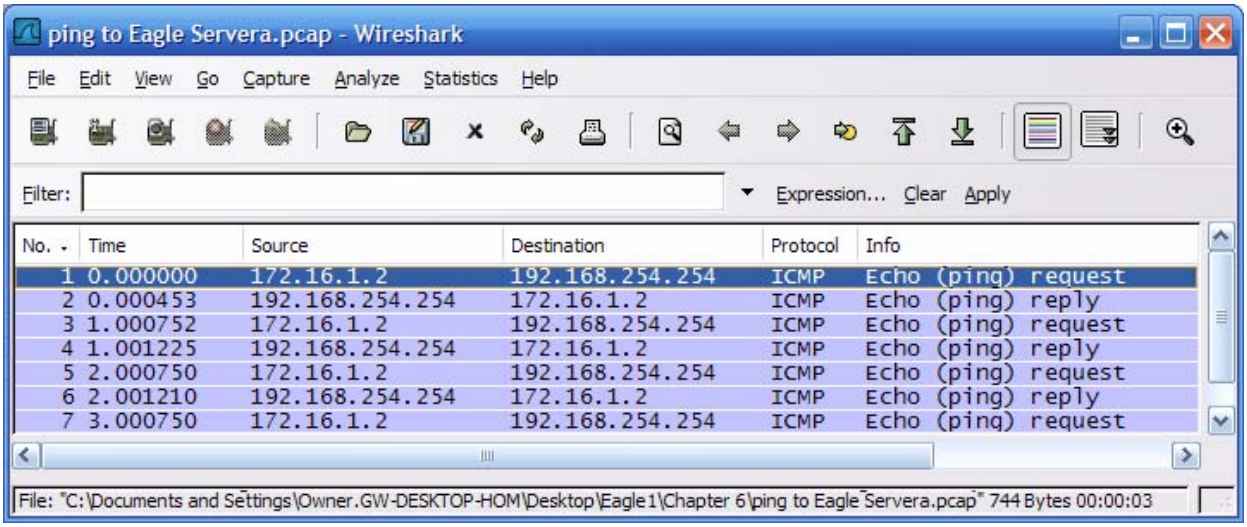


Figura 8. Captura Wireshark de Solicitações e Respostas `ping`

Qual dispositivo de rede responde à solicitação de echo ICMP? _____

5. Expanda a janela do meio no Wireshark e expanda o registro do Internet Control Message Protocol até que todos os campos estejam visíveis. A janela inferior também será necessária para examinar o campo de Dados.
6. Registre as informações do *primeiro* pacote de solicitação de echo ao Eagle Server:

Campo	Valor

Tipo	
Código	
Checksum	
Identificador	
Número de seqüência	
Dados	

Existem 32 bytes de dados? ___

7. Registre informações do *primeiro* pacote de resposta de echo do Eagle Server:

Campo	Valor
Tipo	
Código	
Checksum	
Identificador	
Número de seqüência	
Dados	

Quais campos, se houve, mudaram da solicitação de echo?

_____

Pacote	Checksum	Identificador	Número de seqüência
Solicitação # 2			
Resposta # 2			
Solicitação # 3			
Resposta # 3			
Solicitação # 4			
Resposta # 4			

Por que os valores de Checksum mudaram com cada nova solicitação?

_____

Passo 2: Capturar e avaliar mensagens de echo ICMP para 192.168.253.1

Neste passo, os pings serão enviados a uma rede e um host fictícios. Os resultados da captura Wireshark serão avaliados—e poderão ser surpreendentes.

Tente efetuar ping no endereço IP 192.168.253.1.

```
C:\> ping 192.168.253.1
```



```
C:\> ping 192.168.253.1
Pinging 192.168.253.1 com 32 bytes de dados:
Resposta de 172.16.255.254: Host de destino não alcançável.
Resposta de 172.16.255.254: Host de destino não alcançável.
Resposta de 172.16.255.254: Host de destino não alcançável.
Resposta de 172.16.255.254: Host de destino não alcançável.
Estatísticas de ping para 192.168.253.1:
    Pacotes: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\ >
```

Figura 9. Resultados do Ping de um Destino Fictício

Veja a Figura 9. Ao invés do tempo limite de uma solicitação, há uma resposta de echo.

Qual dispositivo de rede responde a pings para um destino fictício?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

Figura 10. Captura Wireshark de um Destino Fictício

Capturas Wireshark a um destino fictício são as na Figura 10. Expanda a janela do Wireshark do meio e o registro do Internet Control Message Protocol record.

Qual tipo de mensagem ICMP é usado para devolver informações ao remetente?

_____

Qual é o código associado ao tipo de mensagem?

_____

Passo 3: Capturar e avaliar mensagens de echo ICMP que excedem o valor TTL

Neste passo, os pings serão enviados com um baixo valor TTL, simulando um destino inalcançável. Faça o ping no Eagle Server e configure o valor TTL para **1**:

```
C:\> ping -i 1 192.168.254.254
```

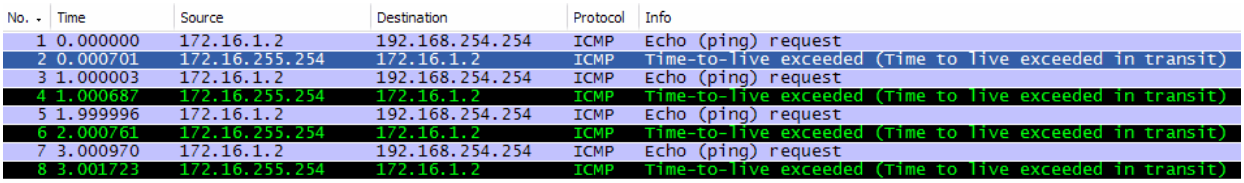
```
C:\> ping -i 1 192.168.254.254
Pinging 192.168.254.254 com 32 bytes de dados:
Resposta de 172.16.255.254: TTL expirou em trânsito.
Resposta de 172.16.255.254: TTL expirou em trânsito.
Resposta de 172.16.255.254: TTL expirou em trânsito.
Resposta de 172.16.255.254: TTL expirou em trânsito.
Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\ >
```

Figura 11. Resultados do Ping para um TTL Excedido

Veja a Figura 11, que mostra respostas ping quando o valor TTL foi excedido.

Qual dispositivo de rede responde a pings que excederam o valor TTL?

_____



No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Figura 12. Captura Wireshark de Valor TTL Excedido

Capturas Wireshark a um destino fictício são as na Figura 12. Expanda a janela do Wireshark do meio e o registro do Internet Control Message Protocol record.

Qual tipo de mensagem ICMP é usado para devolver informações ao remetente?

_____

Qual é o código associado ao tipo de mensagem?

_____

Qual dispositivo de rede é responsável por reduzir o valor TTL?

_____

Tarefa 3: Desafio

Use o Wireshark para capturar um sessão **`tracert`** ao Eagle Server e então ao 192.168.254.251. Examine a mensagem de TTL excedido ICMP. Isso demonstrará como o comando **`tracert`** rastreia o caminho de rede ao destino.

Tarefa 4: Reflexão

O protocolo ICMP é bastante útil para se corrigir problemas de conectividade de rede. Sem as mensagens ICMP, um remetente não tem como dizer por que uma conexão de destino falhou. Usando o comando **`ping`**, diferentes valores de tipo de mensagem ICMP foram capturados e avaliados.

Tarefa 5: Limpeza

O Wireshark pode ter sido instalado no computador. Se o programa deve ser removido, clique em **Iniciar > Painel de Controle > Adicionar ou Remover Programas** e selecione o Wireshark. Clique no nome do arquivo, clique em **Remover** e siga as instruções de desinstalação.

Remova quaisquer arquivos pcap Wireshark que foram criados no computador.

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.

