Solución:Laboratorio 6.7.2: Examen de paquetes ICMP

Diagrama de topología

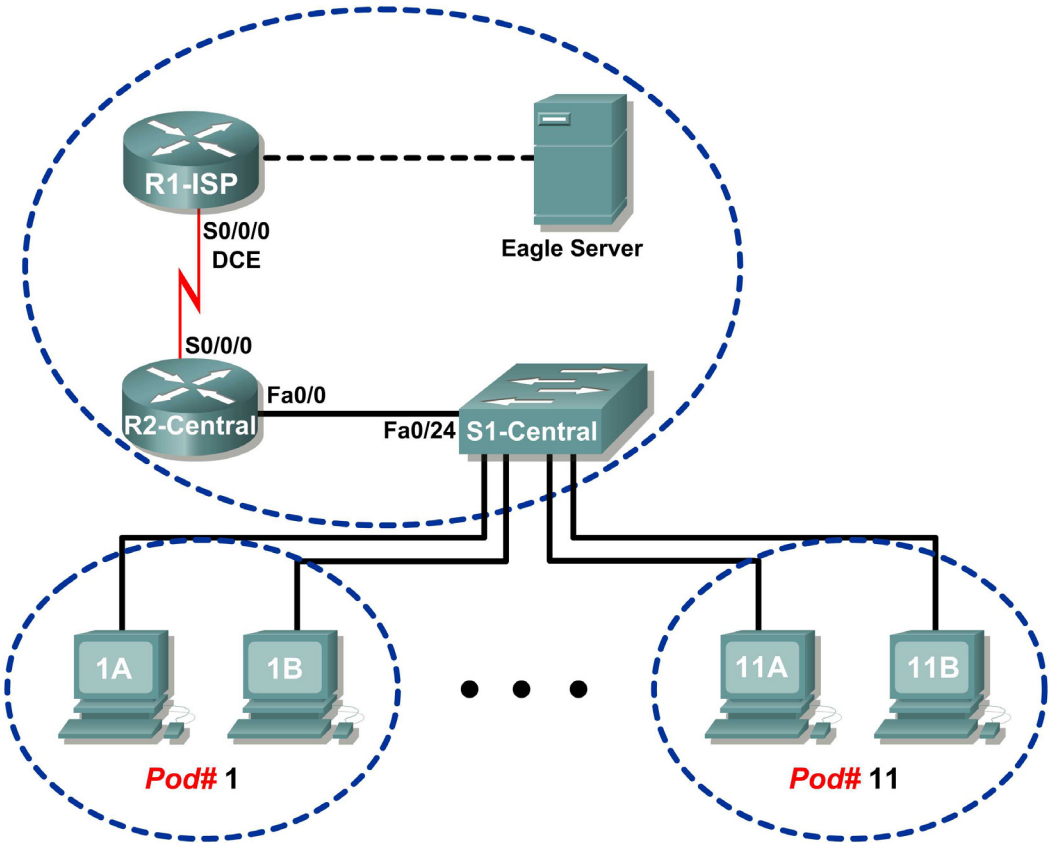


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#*A	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Comprender el formato de los paquetes ICMP.
- Usar Wireshark para capturar y examinar mensajes ICMP.

Información básica

El Internet Control Message Protocol (ICMP) se definió por primera vez en RFC 792, en septiembre de 1981. Los tipos de mensajes ICMP luego se expandieron en RFC 1700. ICMP funciona en la capa de red TCP/IP y se usa para intercambiar información entre dispositivos.

Los paquetes ICMP cumplen muchos usos en la red de computadoras actuales. Cuando un router no puede enviar un paquete al host o a la red de destino, se devuelve un mensaje informativo. Los comandos **ping** y **tracert** también envían mensajes ICMP a los destinos y los destinos responden con mensajes ICMP.

Escenario

Con el laboratorio Eagle 1, las capturas de Wireshark se realizan con paquetes ICMP entre los dispositivos de red.

Tarea 1: Comprensión del formato de paquetes ICMP.

Paquete ICMP: Información de encabezado de mensaje común

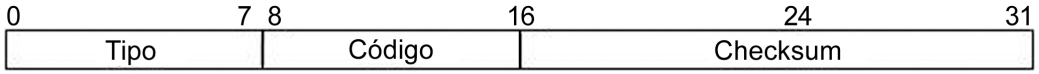


Figura 1. Encabezado de mensajes ICMP

Consulte la figura 1. Los campos de encabezados ICMP son comunes a todos los tipos de mensajes ICMP. Cada mensaje ICMP comienza con un campo Tipo de 8-bits, un campo Código de 8-bits y una Checksum calculada de 16-bits. El tipo de mensaje ICMP describe los campos ICMP restantes. La tabla de la Figura 2 muestra los tipos de mensajes ICMP de RFC 792:

Valor	Significado
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen
5	Redirigir
8	Eco
11	Tiempo superado
12	Problema de parámetros
13	Marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información

Figura 2. Tipos de mensajes ICMP

Los códigos proporcionan información adicional al campo Tipo. Por ejemplo, si el campo Tipo es 3, destino inalcanzable, se devuelve la información adicional sobre el problema al campo Código. La tabla de la Figura 3 muestra los códigos de mensajes para un mensaje Tipo 3 ICMP, destino inalcanzable, de RFC 1700:

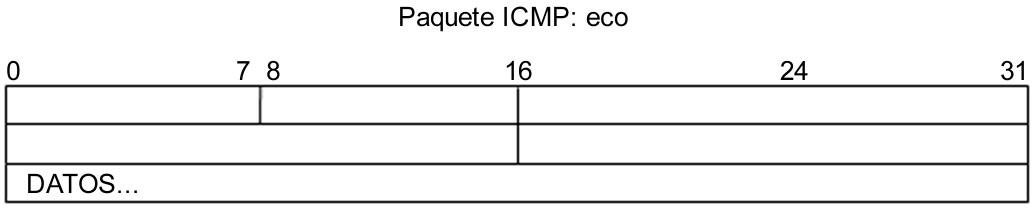
Código Valor	Significado
0	Red inalcanzable
1	Host inalcanzable
2	Protocolo inalcanzable
3	Puerto inalcanzable
4	Se necesita fragmentación y no se configuró un fragmento
5	Falló la ruta origen
6	Red de destino desconocida
7	Host de destino desconocido
8	Host de origen aislado
9	La comunicación con la red de destino se encuentra administrativamente prohibida.
10	La comunicación con el host de destino se encuentra administrativamente prohibida
11	Red de destino inalcanzable para el tipo de servicio
12	Host de destino inalcanzable para el tipo de servicio

Figura 3. Códigos de mensajes ICMP Tipo 3

Complete los campos para la solicitud de eco de paquetes ICMP con la captura de mensajes ICMP que se muestra en la Figura 4. Los valores que comienzan con `0x` son números hexadecimales:

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

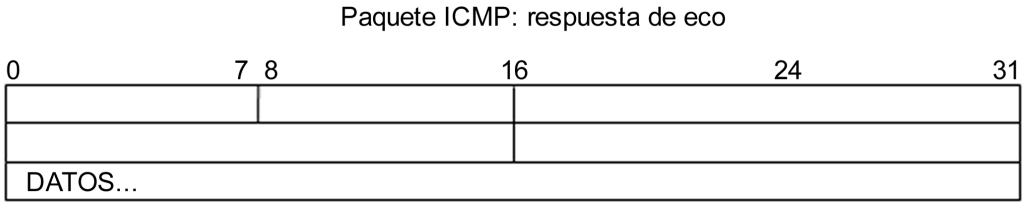
Figura 4. Solicitud de eco de paquetes ICMP



Complete los campos para la respuesta de eco de paquetes ICMP con la captura de mensajes ICMP que se muestra en la Figura 5:

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

Figura 5. Respuesta de eco de paquetes ICMP



En la capa de red TCP/IP no se garantiza la comunicación entre dispositivos. Sin embargo, ICMP sí proporciona controles mínimos para que una respuesta coincida con la solicitud. A partir de la información proporcionada en el mensaje ICMP anteriormente, ¿cómo sabe el emisor que la respuesta es para un eco específico?

Sabemos que se corresponde por el numero de secuencia.

Tarea 2: Utilización de Wireshark para capturar y examinar mensajes ICMP

Figura 6. Sitio de descarga de Wireshark

Si no se ha cargado Wireshark en la computadora host del grupo, se puede descargar desde Eagle Server.

1. Abra un explorador Web, URL FTP://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6, como se muestra en la Figura 6.
2. Haga clic con el botón derecho del mouse sobre el nombre del archivo Wireshark, haga clic en **Guardar enlace como**, y guarde el archivo en la computadora host del grupo.
3. Cuando se haya descargado el archivo, abra e instale Wireshark.

Paso 1: Capturar y evaluar los mensajes de eco ICMP para Eagle Server.

En este paso, Wireshark se usa para examinar los mensajes de eco ICMP.

1. Abra una terminal de Windows en la computadora host del módulo del grupo.
2. Una vez listo, inicie la captura de 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 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<1ms TTL=63
Reply from 192.168.254.254: bytes=32 time<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. Respuestas de `ping` exitosas de Eagle Server

3. Desde la terminal de Windows, haga **`ping`** en Eagle Server. Se deben recibir cuatro respuestas exitosas de Eagle Server, como se muestra en la Figura 7.
4. Detenga la captura de Wireshark. Debe haber un total de cuatro solicitudes de eco ICMP y respuestas eco que coincidan, similares a las que se muestran en la Figura 8.

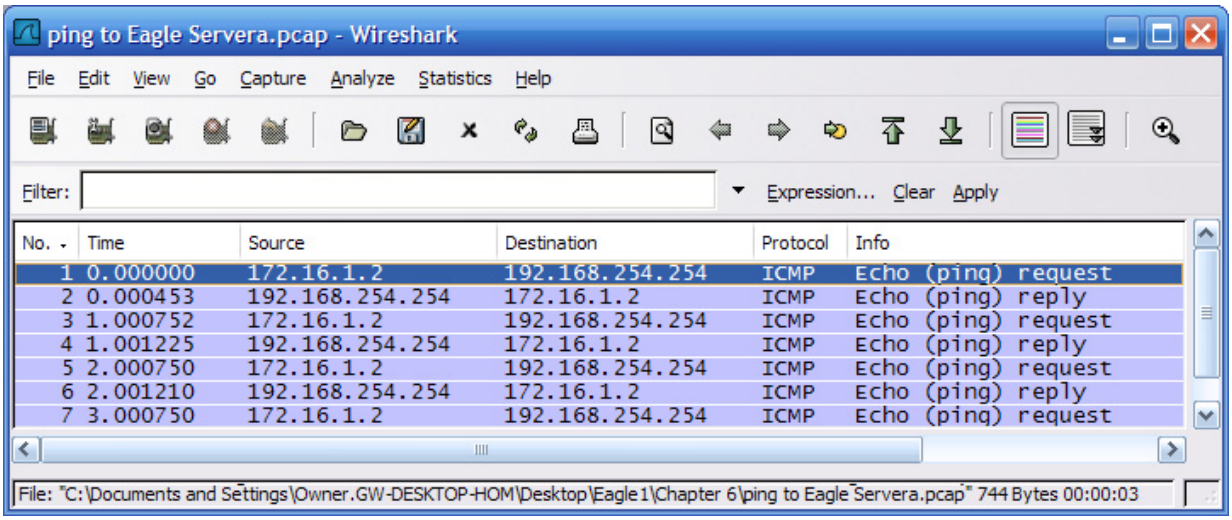


Figura 8. Captura de Wireshark de solicitudes de `ping` y respuestas

¿Qué dispositivo de red responde a la solicitud de eco ICMP? Nos responde el host de destino del ping

5. Expanda la ventana del medio en Wireshark, y expanda el registro de Internet Control Message Protocol hasta que se visualicen todos los campos. También se necesitará la ventana inferior para examinar el campo Datos.
6. Registre la información del *primer* paquete de solicitud de eco a Eagle Server.

Campo	Valor
Tipo	8
Código	0
Checksum	0x015c [correct]
Identificador	(BE): 512 (0x0200) (LE): 2 (0x0002)
Número de secuencia	(BE): 18944 (0x4a00) (LE): 74 (0x004a)
Datos	32 bytes

¿Existen 32 bytes de datos? Si, los vemos en la trama

7. Registre la información del *primer* paquete de respuesta de eco de Eagle Server:

Campo	Valor
Tipo	0
Código	0
Checksum	0x095c [correct]
Identificador	(BE): 512 (0x0200) (LE): 2 (0x0002)
Número de secuencia	(BE): 18944 (0x4a00) (LE): 74 (0x004a)
Datos	32 bytes

¿Qué campos, de haber alguno, cambian desde la solicitud de eco?

El Tipo y el Checksum

8. Continúe evaluando las solicitudes y respuestas de eco restantes. Complete la siguiente información de cada ping nuevo:

Paquete	Checksum	Identificador	Número de secuencia
Solicitud N.º 2	0x005c	(BE) 512(LE)2	(BE)19200(LE)75
Respuesta N.º 2	0x085c	(BE) 512(LE)2	(BE)19200(LE)75
Solicitud N.º 3	0xff5b	(BE) 512(LE)2	(BE)19456(LE)76
Respuesta N.º 3	0x075c	(BE) 512(LE)2	(BE)19456(LE)76
Solicitud N.º 4	0xfe5b	(BE) 512(LE)2	(BE)19712(LE)77
Respuesta N.º 4	0x065c	(BE) 512(LE)2	(BE)19712(LE)77

¿Por qué cambiaron los valores de Checksum con cada nueva solicitud?
Por que en cheksum se guarda el resultado de hacer una operacion con todoslos datos de la trama, y siempre cambia algo con lo cual el resultado es diferente.

Paso 2: Capturar y evaluar los mensajes de eco ICMP a 192.168.253.1.

En este paso, los pings se envían a un host y red ficticios. Los resultados de captura de Wireshark se evaluarán, y pueden ser sorprendentes.

Intente hacer ping en la dirección IP 192.168.253.1.

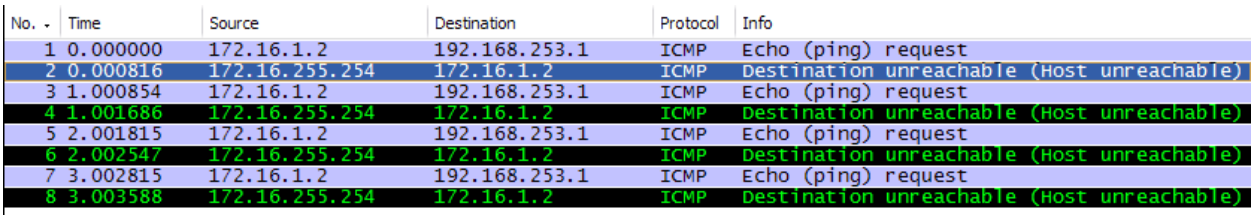
```
C:\> ping 192.168.253.1
```

```
C:\> ping 192.168.253.1
Pinging 192.168.253.1 with 32 bytes of data:
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Reply from 172.16.255.254: Host de destino inalcanzable.
Ping statistics for 192.168.253.1:
    Packets: 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 de pings de un destino ficticio

Vea la Figura 9. En lugar del límite de tiempo de la solicitud, hay una respuesta de eco.

¿Qué dispositivo de red responde a pings para un destino ficticio? La puerta de enlace



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 de Wireshark de un destino ficticio

Las capturas de Wireshark a un destino ficticio se muestran en la Figura 10. Expanda la ventana Wireshark del medio y el registro de Internet Control Message Protocol.

¿Qué tipo de mensaje ICMP se usa para devolver información al emisor?

Tipo 3, Destination unreachable (host unreachable)

¿Cuál es el código asociado con el tipo de mensaje?

Codigo 1

Paso 3: Capturar y evaluar los mensajes de eco ICMP que exceden el valor TTL.

En este paso, se envían pings con un valor TTL bajo, simulando un destino que es inalcanzable. Haga ping en Eagle Server y establezca el valor TTL para **1**:

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

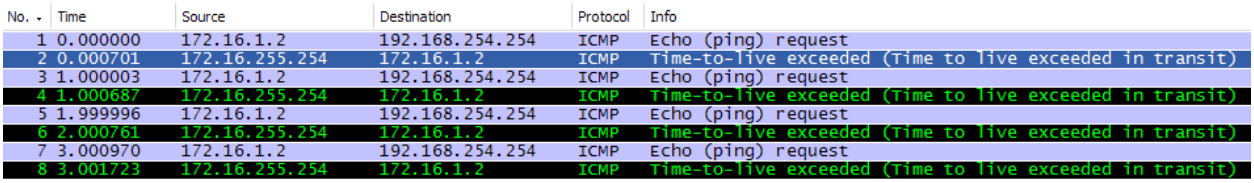
```
C:\> ping -i 1 192.168.254.254
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Reply from 172.16.255.254: TTL expired in transit.
Ping statistics 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 de pings para un TTL excedido

Vea la Figura 11, que muestra respuestas de ping cuando el valor de TTL ha sido superado.

¿Qué dispositivo de red responde a pings que superaron el valor de TTL?

La puerta de enlace



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 del valor de TTL excedido

Las capturas de Wireshark a un destino ficticio se muestran en la Figura 12. Expanda la ventana Wireshark del medio y el registro de Internet Control Message Protocol.

¿Qué tipo de mensaje ICMP se usa para devolver información al emisor?

Tipo 11,Time -to-live exceeded

¿Cuál es el código asociado con el tipo de mensaje?

Codigo 0

¿Qué dispositivo de red es responsable de la disminución del valor de TTL?

Los routers, por cada router que pasa el paquete este le decontara 1 al valor del TTL

Tarea 3: Desafío

Utilice Wireshark para capturar una sesión **`tracert`** para Eagle Server y luego para 192.168.254.251. Examine el mensaje de TTL ICMP superado. Esto demuestra cómo el comando **`tracert`** rastrea la ruta de red hacia el destino.

Tarea 4: Reflexión

El protocolo ICMP es muy útil al resolver problemas relacionados con la conectividad de red. Sin los mensajes ICMP, un emisor no tiene forma de informar porqué falló una conexión de destino. Se capturaron y evaluaron diferentes valores de tipos de mensajes ICMP con el comando **`ping`**.

Tarea 5: Limpieza

Wireshark pudo haber sido cargado en la computadora host del módulo del grupo. Si se debe eliminar el programa, haga clic en **Inicio > Panel de control > Agregar o quitar programas,** desplácese por la pantalla hasta llegar a Wireshark. Haga clic en el nombre del archivo, luego en **Quitar** y siga las instrucciones para desinstalar el programa.

Elimine cualquier archivo pcap de Wireshark que haya sido creado en la computadora host del módulo del grupo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.

