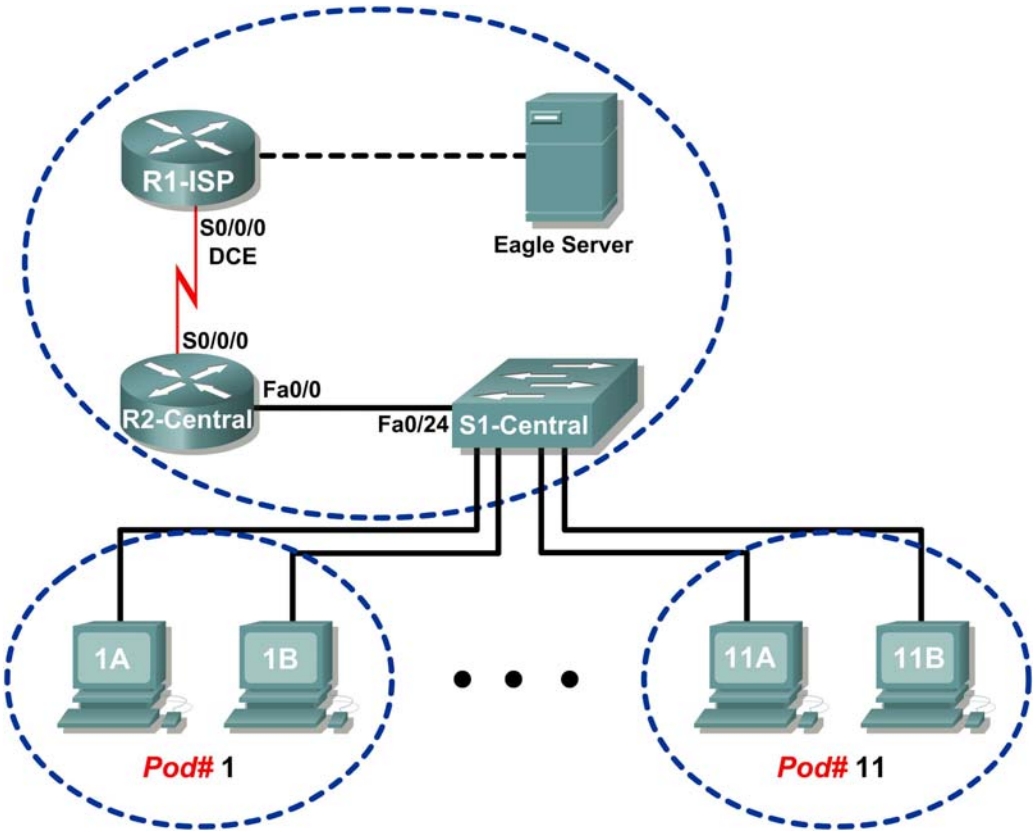
实验 6.7.2：研究 ICMP 数据包

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	不适用
	Fa0/0	192.168.254.253	255.255.255.0	不适用
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	不适用
	Fa0/0	172.16.255.254	255.255.0.0	不适用
Eagle Server	不适用	192.168.254.254	255.255.255.0	192.168.254.253
	不适用	172.31.24.254	255.255.255.0	不适用
host*Pod#*A	不适用	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	不适用	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	不适用	172.16.254.1	255.255.0.0	172.16.255.254

学习目标

完成本实验后，您将能够：

- 了解 ICMP 数据包的格式。
- 使用 Wireshark 捕获和检查 ICMP 消息。

背景

Internet 控制消息协议 (ICMP) 于 1981 年 9 月在 RFC 792 中首次定义，后来在 RFC 1700 中扩充了 ICMP 消息类型。ICMP 在 TCP/IP 网络层运作，用于在设备之间交换信息。

ICMP 数据包在当今计算机网络中发挥着诸多作用。当路由器无法将数据包传送到目的网络或目的主机时，会向源主机返回一则消息。同样，**ping** 和 **tracert** 命令向目的设备发送 ICMP 消息，目的设备也用 ICMP 消息做出响应。

场景

使用 Eagle 1 实验，Wireshark 将捕获网络设备之间的 ICMP 数据包。

任务 1：了解 ICMP 数据包的格式。

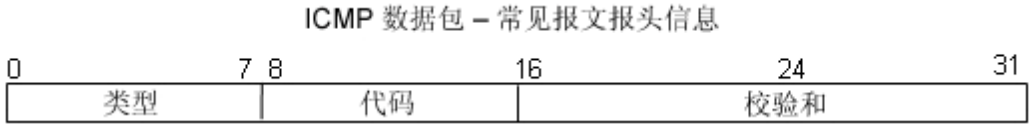


图 1. ICMP 消息的报头

参阅图 1，所有 ICMP 消息类型的 ICMP 报头字段都相同。每个 ICMP 消息均以 8 位“类型”字段开始，然后是 8 位“代码”字段和算出的 16 位“校验和”字段。ICMP 消息的类型说明了其余两个 ICMP 字段。图 2 中的表格显示了 RFC 792 规定的 ICMP 消息类型：

值	含义
0	应答
3	目的无法到达
4	源抑制
5	重定向
8	回应
11	超时
12	参数问题
13	时间戳
14	时间戳应答
15	信息请求
16	信息应答

图 2. ICMP 消息的类型

代码提供了“类型”字段的详细信息。例如，若“类型”字段为 3，则“代码”字段中将返回有关该问题的详细信息。图 3 中的表格显示了 RFC 1700 规定的 ICMP 类型 3 消息（即目的无法到达）的消息代码。

代码值	含义
0	网络无法到达
1	主机无法到达
2	协议无法到达
3	端口无法到达
4	设置了需要分片和不分片
5	源路由失败
6	目的网络未知
7	目的主机未知
8	源主机隔离
9	与目的网络的通信受到管理性禁止
10	与目的主机的通信受到管理性禁止
11	目的网络的服务类型无法到达
12	服务类型的目的主机无法到达

图 3. ICMP 类型 3 消息的代码

使用图 4 所示的 ICMP 消息捕获结果，填写 ICMP 回应请求数据包的字段。以 0x 开头的值是十六进制数字：

```
Internet 控制消息协议
   类型：8（回应 (ping) 请求）
   代码： 0
   校验和：0x365c [正确]
   标识符：0x0200
   序列号：0x1500
   数据（32 字节）
```

图 4. ICMP 回应请求数据包

使用图 5 所示的 ICMP 消息捕获结果，填写 ICMP 应答数据包的字段：

```
Internet 控制消息协议
  类型：8（应答 (ping)）
  代码： 0
  校验和：0x365c [正确]
  标识符：0x0200
  序列号：0x1500
  数据（32 字节）
```

图 5. ICMP 应答数据包

在 TCP/IP 网络层，设备之间的通信不保证送达。但是，ICMP 仍对应答是否与请求相符提供最低检查。根据以上 ICMP 消息中提供的信息回答，发送方如何知道应答是对某个特定回应请求的答复？

_____

_____

任务 2：使用 Wireshark 捕获和检查 ICMP 消息。

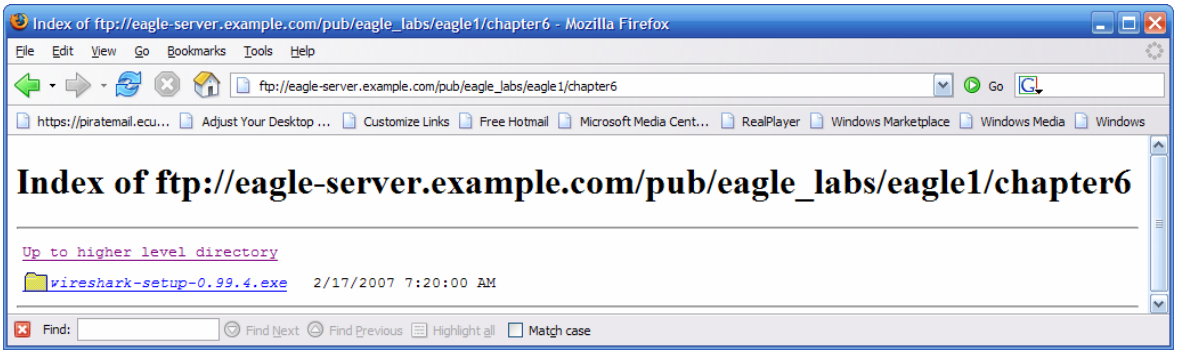


图 6. Wireshark 下载站点

如果 Pod 主机计算机上尚未加载 Wireshark，可以从 Eagle Server 下载。

1. 如图 6 所示，打开 Web 浏览器并输入 URL FTP://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6。
2. 右键单击 Wireshark 文件名，单击 **Save Link As（链接另存为）**，然后将该文件保存到 Pod 主机计算机中。
3. 文件下载完成后，打开文件并安装 Wireshark。

步骤 1：捕获并评估发往 Eagle Server 的 ICMP 回应消息。

此步骤将使用 Wireshark 检查 ICMP 回应消息。

1. 打开 Pod 主机计算机上的 Windows 终端。
2. 准备就绪后，开始 Wireshark 捕获。

```
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:\>
```

图 7. 来自 Eagle Server 的成功 ping 应答

3. 从 Windows 终端 **ping** Eagle Server。应该如图 7 所示从 Eagle Server 收到四个成功的应答。
4. 停止 Wireshark 捕获。总计应有四个 ICMP 回应请求和相应的应答，类似图 8 所示。

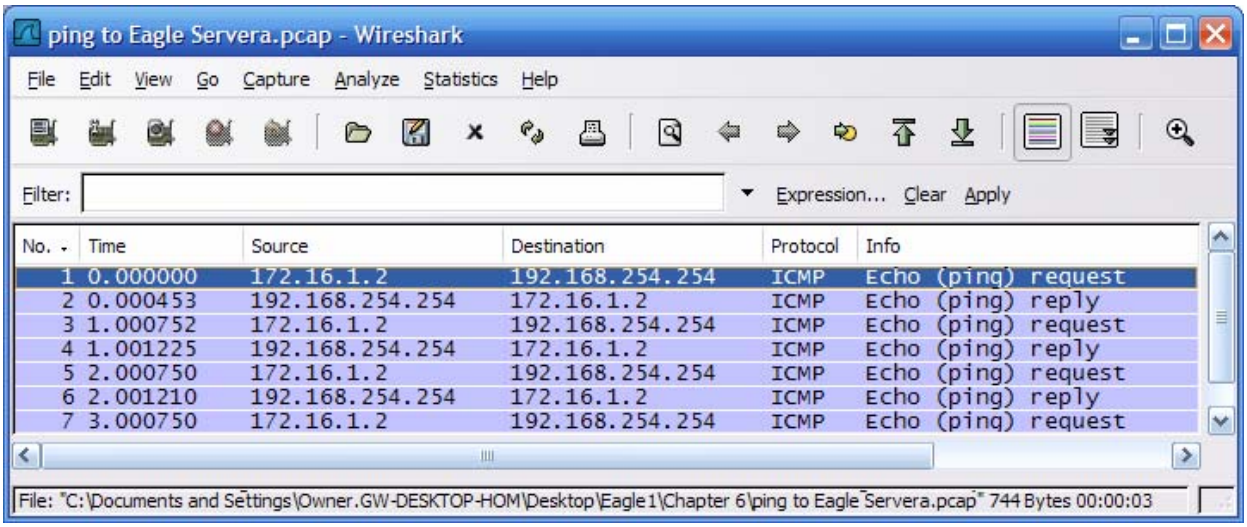


图 8. ping 请求和 ping 应答的 Wireshark 捕获结果

哪台网络设备对 ICMP 回应请求做出了响应？_____

5. 展开 Wireshark 中部窗口，然后展开 Internet 控制消息协议记录，直到显示所有字段。此外还需要检查底部窗口中的“数据”字段。

6. 记录发往 Eagle Server 的*第一个*回应请求数据包的信息。

字段	值
类型	
代码	
校验和	
标识符	
序列号	
数据	

是否有 32 个字节的数据？_____

7. 记录来自 Eagle Server 的*第一个*应答数据包的信息。

字段	值
类型	
代码	
校验和	
标识符	
序列号	
数据	

哪些字段（如果有）与回应请求不同？

_____

8. 继续评估其余回应请求和应答。填写每次新的 ping 操作的下列信息：

数据包	校验和	标识符	序列号
请求 # 2			
应答 # 2			
请求 # 3			
应答 # 3			
请求 # 4			
应答 # 4			

为什么“校验和”的值随着每个新请求而变化？

_____

步骤 2：捕获并评估发往 192.168.253.1 的 ICMP 回应消息。

在此步骤中，ping 将发送到虚构的网络和主机。我们将评估 Wireshark 捕获的结果，答案可能出乎您的意料。

尝试 ping IP 地址 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: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
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:\>
```

图 9. Ping 虚构目的地址的结果

参阅图 9。结果并非请求超时，而是收到了响应。

哪台网络设备对我们向虚构目的地址发出的 ping 做出了响应？

_____

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)

图 10. 虚构目的地址的 Wireshark 捕获

对虚构目的地址的 Wireshark 捕获结果如图 10 所示。展开 Wireshark 中部窗口和 Internet 控制消息协议记录。

哪种 ICMP 消息类型用于向发送方返回信息？

_____

该消息类型的相关代码是什么？

_____

步骤 3：捕获并评估超出 TTL 值的 ICMP 回应消息。

此步骤将发送 TTL 值设置得极低的 ping，模拟无法到达的目的地址。Ping Eagle Server，并将 TTL 值设置为 **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:\>
```

图 11. TTL 超出设置值的 Ping 结果

参阅图 11，图中显示了超出 TTL 值时的 ping 应答。

对超出 TTL 值的 ping 做出响应的是哪台网络设备？

_____

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)

图 12. 超出 TTL 值的 Wireshark 捕获

对虚构目的地址的 Wireshark 捕获结果如图 12 所示。展开 Wireshark 中部窗口和 Internet 控制消息协议记录。

哪种 ICMP 消息类型用于向发送方返回信息？

_____

该消息类型的相关代码是什么？

_____

哪台网络设备负责扣减 TTL 值？

_____

任务 3：练习

使用 Wireshark 捕获与 Eagle Server 和 192.168.254.251 之间的 **tracert** 会话。检查超出 TTL 值的 ICMP 消息。本练习将演示 **tracert** 命令如何跟踪通往目的地址的网络路径。

任务 4：思考

ICMP 协议在排除网络连接问题时非常实用。如果没有 ICMP 消息，发送方就无从了解目的连接失败的原因。使用 **ping** 命令可以捕获并评估不同 ICMP 消息类型的值。

任务 5：课后清理

Pod 主机计算机上可能已加载了 Wireshark。如果必须删除该程序，请单击**开始 > 控制面板 > 添加或删除程序**，然后向下滚动到 Wireshark。单击该文件名，单击**删除**，然后按照卸载说明操作。

删除 Pod 主机计算机上创建的任何 Wireshark pcap 文件。

除非教师另有指示，否则请关闭主机计算机的电源。带上您带进实验室的所有物品离开，将实验室留给下一班同学。