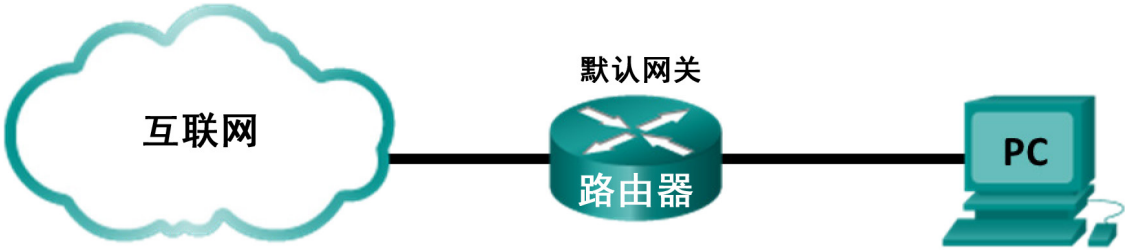
实验 – 使用 Wireshark 检查以太网帧

拓扑



目标

第 1 部分：检查以太网 II 帧中的报头字段

第 2 部分：使用 Wireshark 捕获和分析以太网帧

背景/场景

当上层协议互相通信时，数据会向下流到开放式系统互联 (OSI) 层，并且封装入第 2 层帧。帧的成分取决于介质访问类型。例如，如果上层协议是 TCP 和 IP 并且介质访问是以太网，则第 2 层帧的封装为以太网 II。这是 LAN 环境的典型情况。

在了解第 2 层的概念时，分析帧报头信息很有帮助。在此实验的第 1 部分，您将查看以太网 II 帧包含的字段。在第 2 部分中，您可以使用 Wireshark 捕获和分析以太网 II 帧头字段，以区分本地和远程流量。

所需资源

- 1 台 PC（采用 Windows 7 或 8 且可访问互联网，并且已安装 Wireshark）

第 1 部分：检查以太网 II 帧中的报头字段

在第 1 部分中，您需要检查以太网 II 帧中的报头字段和内容。使用 Wireshark 捕获检查这些字段中的内容。

第 1 步：检查以太网 II 帧头字段描述和长度。

前导码	目的地址	源地址	帧类型	数据	FCS
8 个字节	6 个字节	6 个字节	2 个字节	46 – 1500 个字节	4 个字节

第 2 步： 检查 PC 的网络配置。

该 PC 的主机 IP 地址为 192.168.1.17，默认网关的 IP 地址为 192.168.1.1。

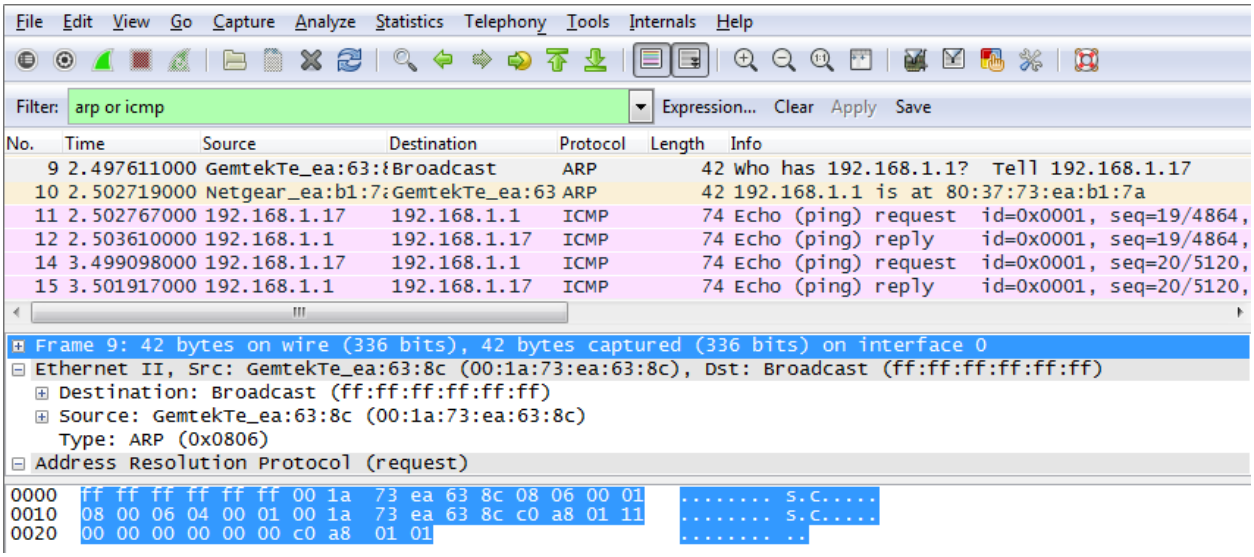
```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11a/b/g WLAN
   Physical Address. . . . . . . . . : 00-1A-73-EA-63-8C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 16, 2015 6:59:54 AM
   Lease Expires . . . . . . . . . . : Wednesday, June 17, 2015 6:59:54 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234887795
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-07-0A-E1-00-1E-EC-15-74-C2

   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

第 3 步： 检查 Wireshark 捕获中的以太网帧。

以下 Wireshark 捕获显示了从 PC 主机发送到默认网关的 ping 生成的数据包。已对 Wireshark 应用过滤器，以仅查看 ARP 和 ICMP 协议。会话首先利用 ARP 查询网关路由器的 MAC 地址，然后是四次 ping 请求和应答。



第 4 步： 检查 ARP 请求的以太网 II 报头内容。

下表使用 Wireshark 捕获中的第一个帧，并显示以太网 II 帧头字段中的数据。

字段	价值	描述
前导码	捕获中未显示	此字段包含同步比特，由网卡硬件处理。
目的地址	广播 (ff:ff:ff:ff:ff:ff)	帧的第 2 层地址。每个地址的长度都是 48 位或 6 个二进制八位数，表示为 12 个十六进制数字：0-9、A-F。常用格式为 12:34:56:78:9A:BC。 前六个十六进制数字表示网络接口卡 (NIC) 的制造商，后六个十六进制数字是网卡的序列号。 目的地址可能是全部为 1 的广播地址，也可能是单播地址。源地址始终是单播地址。
源地址	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)	
帧类型	0x0806	对于以太网 II 帧，此字段包含用来在数据字段中表示上层协议类型的十六进制值。以太网 II 支持多个上层协议。两种常用的帧类型为： 值 说明 0x0800 IPv4 协议 0x0806 地址解析协议 (ARP)
数据	ARP	包含封装的上层协议。数据字段在 46 – 1,500 个字节之间。
FCS	捕获中未显示	帧校验序列 (FCS)，供网卡用来查找传输过程中的错误。其值包含帧地址、类型和数据字段，由发送方计算，由接收方验证。

关于目的地址字段的内容，需要注意什么？

为什么 PC 会在发送第一个 ping 请求之前发送广播 ARP？

第一个帧的源设备的 MAC 地址是什么？

源设备的网卡的供应商 ID (OUI) 是什么？

MAC 地址的哪个部分是 OUI？

源设备的网卡序列号是什么？

第 2 部分：使用 Wireshark 捕获和分析以太网帧

在第 2 部分中，您将使用 Wireshark 捕获本地和远程以太网帧。然后您将检查帧头字段中包含的信息。

第 1 步：确定 PC 上的默认网关的 IP 地址。

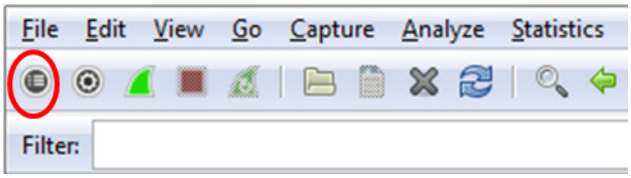
打开命令提示符窗口并发出 **ipconfig** 命令。

PC 默认网关的 IP 地址是多少？

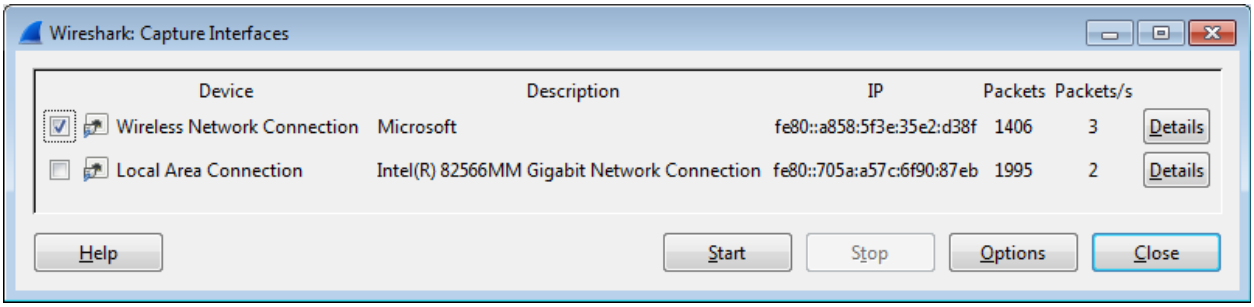
第 2 步： 开始捕获 PC 网卡上的流量。

a. 打开 Wireshark。

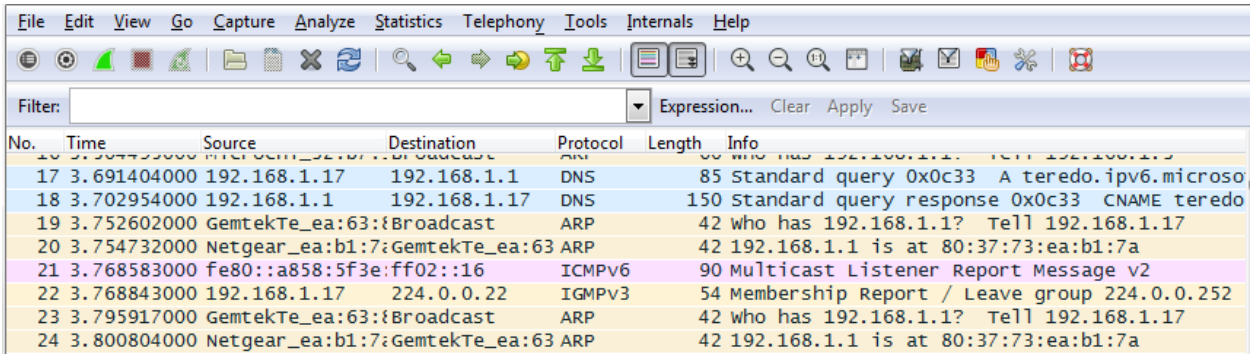
b. 在 Wireshark Network Analyzer 工具栏上，单击 **Interface List**（接口列表）图标。



c. 在“Wireshark: Capture Interfaces”（Wireshark：捕获接口）窗口中，单击相应的复选框选择要开始捕获流量的接口，然后单击 **Start**（开始）。如果您不确定选中哪个接口，请单击 **Details**（详细信息）了解列出的每个接口的详细信息。



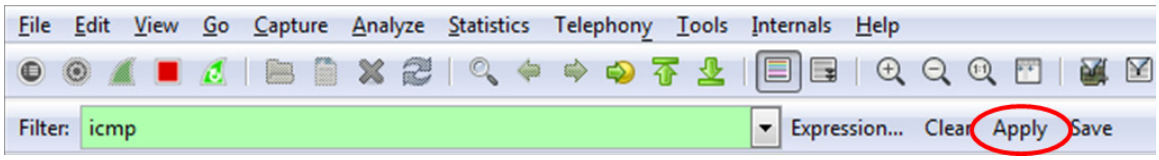
d. 观察“Packet List”（数据包列表）窗口中显示的流量。



第 3 步： 过滤 Wireshark，以仅显示 ICMP 流量。

您可以使用 Wireshark 中的过滤器拦截不需要的流量。过滤器不会拦截非需要数据的捕获，它只过滤屏幕上显示的数据。现在，屏幕只会显示 ICMP 流量。

在 Wireshark 的 **Filter**（过滤器）框中，键入 **icmp**。如果您正确键入过滤器，方框应会变为绿色。如果方框变为绿色，则单击 **Apply**（应用）应用过滤器。

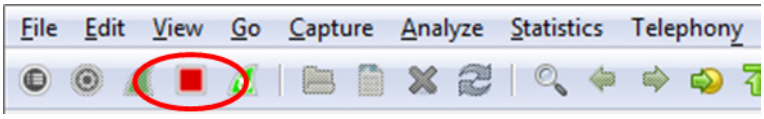


第 4 步： 在命令提示符窗口中，对 PC 的默认网关执行 ping 操作。

从命令窗口中，使用您在第 1 步中记录的 IP 地址对默认网关执行 ping 操作。

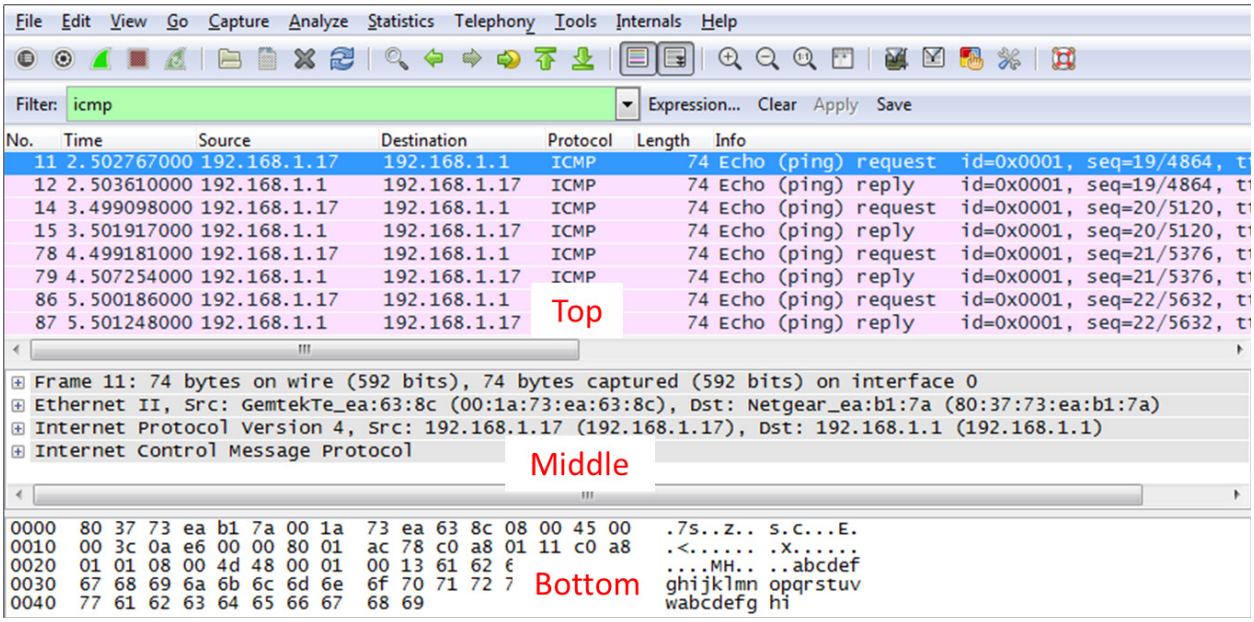
第 5 步： 停止捕获网卡上的流量。

单击 **Stop Capture**（停止捕获）图标停止捕获流量。



第 6 步： 检查 Wireshark 中的第一个响应 (ping) 请求。

Wireshark 主窗口分为三个部分：数据包列表窗格（上）、数据包详细信息窗格（中）和数据包字节窗格（下）。如果您在第 3 步中选择了正确的接口来捕获数据包，Wireshark 将在 Wireshark 的数据包列表窗格中显示 ICMP 信息，类似于以下示例。



a. 在数据包列表窗格中（上面部分），单击列出的第一个帧。您应该会在 **Info**（信息）标题下看到 **Echo (ping) request**（响应 (ping) 请求）。应该会用蓝色突出显示。

b. 检查数据包详细信息窗格（中间部分）中的第一行。该行显示帧的长度；此示例中为 74 字节。

c. 数据包详细信息窗格中的第二行显示这是一个以太网 II 帧。还会显示源 MAC 地址和目的 MAC 地址。

PC 网卡的 MAC 地址是什么？

默认网关的 MAC 地址是什么？

d. 您可以单击第二行开头处的加号 (+) 以获取关于以太网 II 帧的详细信息。注意加号会变成减号 (-)。

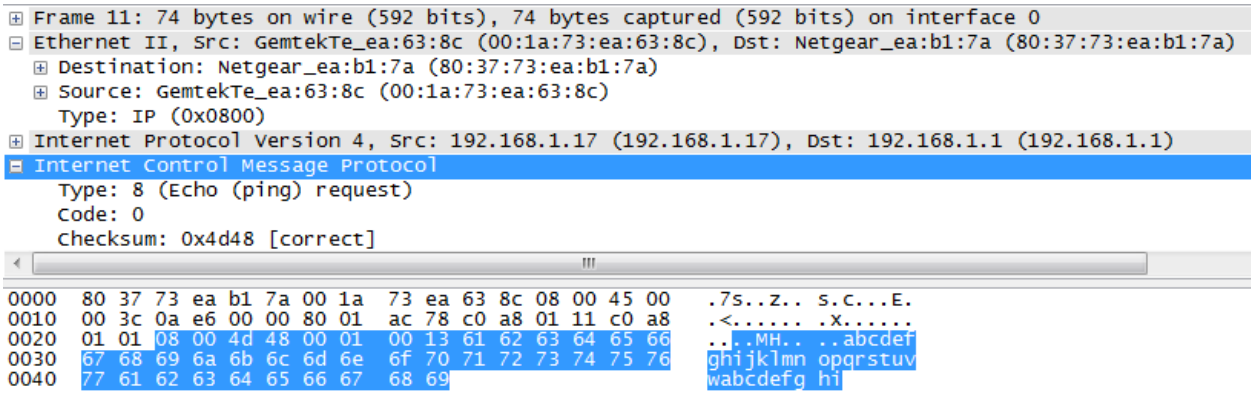
显示的是哪种帧？

e. 中间部分显示的最后两行显示关于帧的数据字段的信息。注意数据包含源和目的 IPv4 地址信息。

源 IP 地址是什么？

目的 IP 地址是什么？

f. 您可以单击中间部分的任意一行，在数据包字节窗格（下面部分）中突出显示帧（十六进制和 ASCII）的这一部分。单击中间部分的 **Internet Control Message Protocol**（互联网控制消息协议）行，检查数据包字节窗格中突出显示的内容。



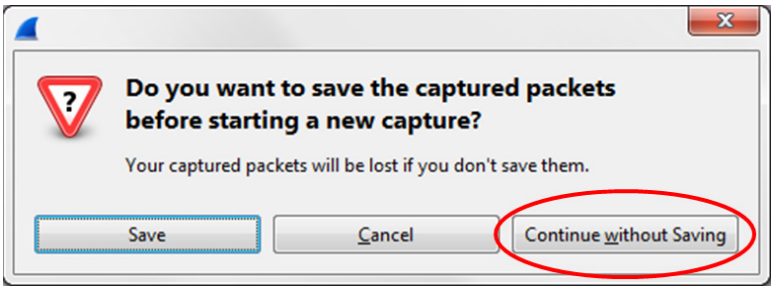
最后两个突出显示的二进制八位数怎么读？

g. 单击上面部分中的下一个帧，并检查响应应答帧。注意源和目的 MAC 地址的顺序颠倒了，因为该帧是默认网关路由器发出的，是对第一个 ping 的应答。

哪个设备和 MAC 地址显示为目的地址？

第 7 步： 在 Wireshark 中重新开始数据包捕获。

单击 **Start Capture**（开始捕获）图标开始新的 Wireshark 捕获。在开始新的捕获之前，您将看到一个弹出窗口，询问您是否将之前捕获的数据包保存到文件中。单击 **Continue without Saving**（继续但不保存）。



第 8 步： 在命令提示符窗口中，对 www.cisco.com 执行 ping 操作。

第 9 步： 停止捕获数据包。

第 10 步: 检查 Wireshark 数据包列表窗格中的新数据。

在第一个响应 (ping) 请求帧中，源和目的 MAC 地址是什么？

源：

目的：

帧的数据字段包含哪个源和目的 IP 地址？

源：

目的： _____

比较这些地址与您在第 6 步中接收到的地址。只有目的 IP 地址发生变化。为什么目的 IP 地址发生变化，而目的 MAC 地址保持不变？

思考

Wireshark 不显示帧头的前导码字段。前导码包含什么？