实验 11.5.6：最终案例研究 — 使用 Wireshark 分析数据报

学习目标

完成本练习之后，学生将能够演示：

- TCP 数据段的构建过程，并能解释数据段的各个字段。
- IP 数据包的构建过程，并能解释数据包的各个字段。
- Ethernet II 帧的构建过程，并能解释帧的各个字段。
- ARP 请求和 ARP 回应的内容。

背景

此实验需要两个捕获的数据包文件以及网络协议分析程序 Wireshark。从 Eagle 服务器下载下列文件，如果您的电脑尚未安装 Wireshark，请安装。

- eagle1_web_client.pcap（讨论对象）
- eagle1_web_server.pcap（仅供参考）
- wireshark.exe

场景

本练习详细讨论创建数据报并将其通过网络在 web 客户端 PC_Client 与 web 服务器 eagle1.example.com 之间传输的序列。理解循序渐进地将数据包放到网络上的过程后，学生可在出现网络连接故障时从逻辑上排除故障。为简洁明了起见，捕获过程中的网络数据包噪音被忽略。当您在别人的网络上执行网络协议分析之前，请确保获得书面许可。

图 1 所示为本实验的拓扑。

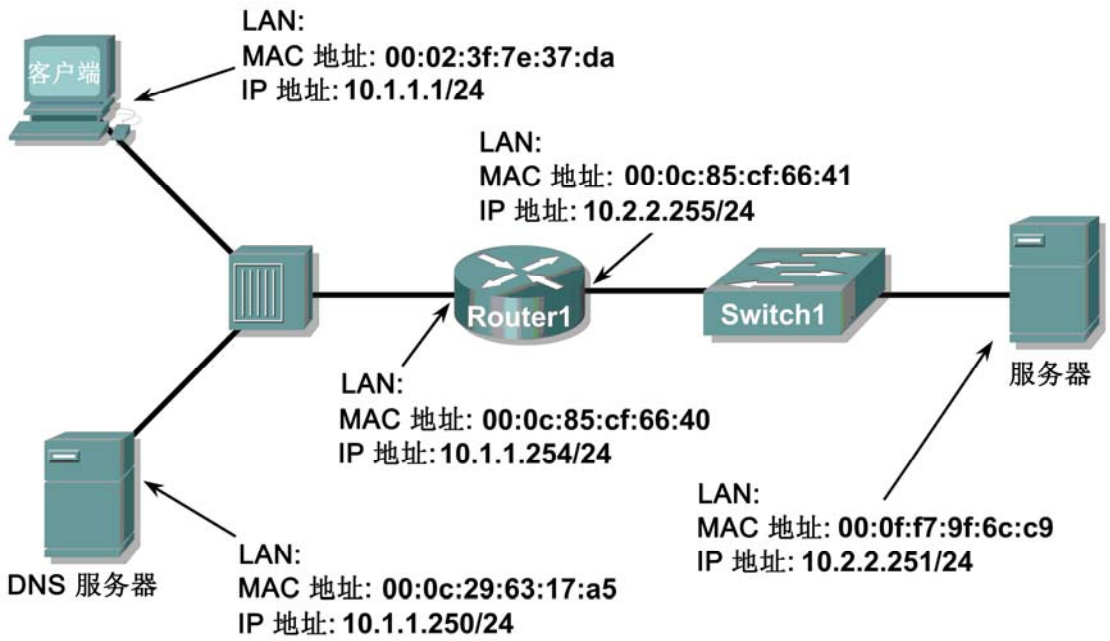

图 1. 网络拓扑。

使用 Microsoft ® 命令行工具将 IP 配置信息和 ARP 缓存内容显示如下。请参阅图 2。

```
C: > ipconfig / all
Windows IP Configuration
Ethernet adapter Local Area Connection:
     Connection-specific DNS Suffix  . :
     Description . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                          Network Connection
     Physical Address. . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp Enabled. . . . . . . . . . . : No
     IP Address. . . . . . . . . . . . : 10.1.1.1
     Subnet Mask . . . . . . . . . . . : 255.255.255.0
     Default Gateway . . . . . . . . . : 10.1.1.254
     DNS Servers . . . . . . . . . . . : 10.1.1.250
C: > arp –a
No ARP Entries Found
C: >
```

图 2. PC 客户端初始网络状态。

如图 3 所示，已启动一个 web 客户端并输入了 URL eagle1.example.com。这将启动与该 web 服务器的通信过程，且数据包捕获即从此处开始。

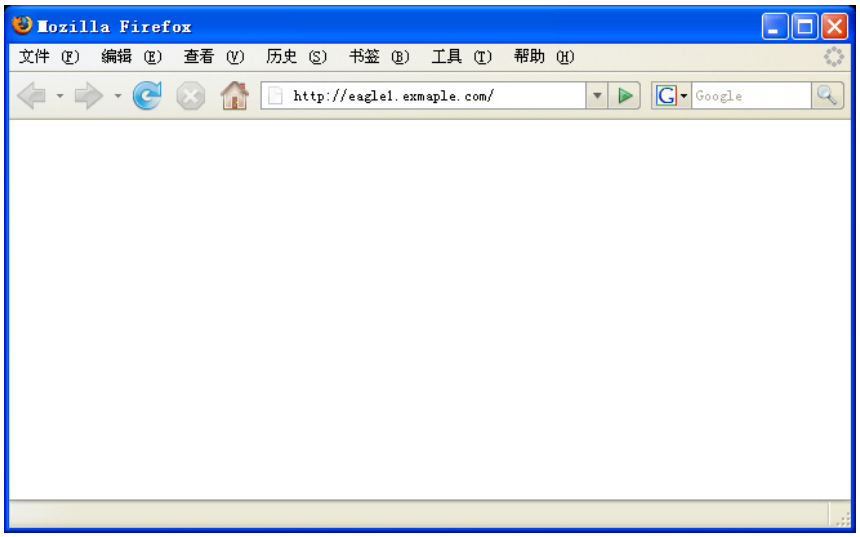

图 3. 带有 web 浏览器的 PC 客户端。

任务 1：准备实验。

步骤 1：在您的计算机上启动 Wireshark。

请参阅图 4 更改默认输出。取消选择 Main toolbar（主工具栏）、Filter toolbar（过滤器工具栏）和 Packet Bytes（数据包字节数）。确保选中 Packet List（数据包列表）和 Packet Details（数据包详细信息）。为确保不自动转换 MAC 地址，请取消选择 MAC layer（MAC 层）和 Transport Layer（传输层）的 Name Resolution（名称解析）。

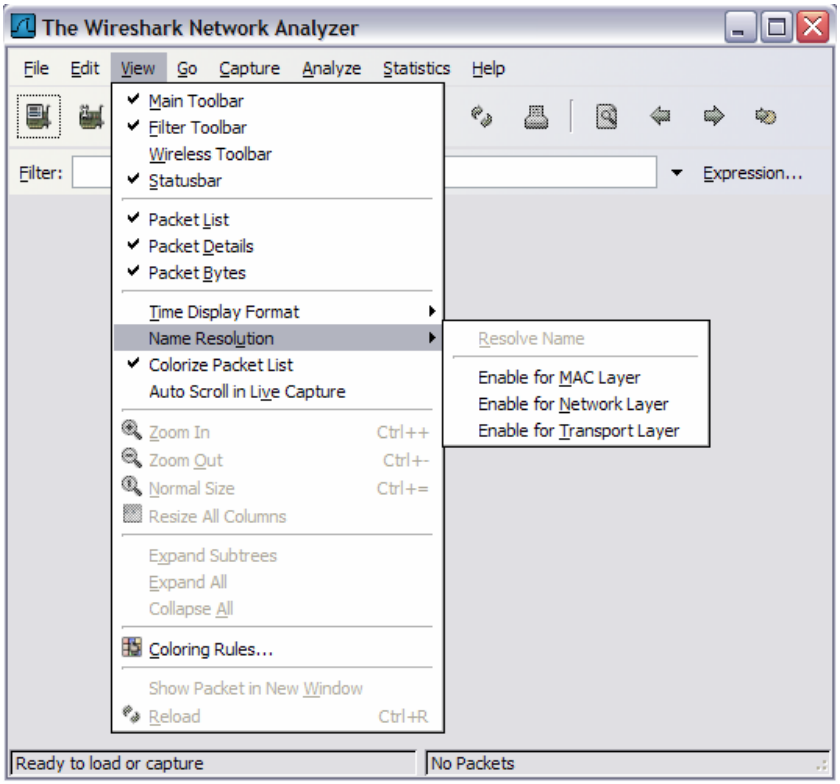

图 4. 更改 Wireshark 的默认视图。

步骤 2：加载 web 客户端捕获文件 `eagle1_web_client.pcap`。

将出现类似图 5 的画面。其中提供了多种下拉菜单和子菜单。还有两个单独的数据窗口。上方的 Wireshark 窗口列出了捕获的所有数据包。下方的窗口包含数据包的详细信息。在下方的窗口中，如果行首带有复选框 ☒，则表示提供有更多信息。

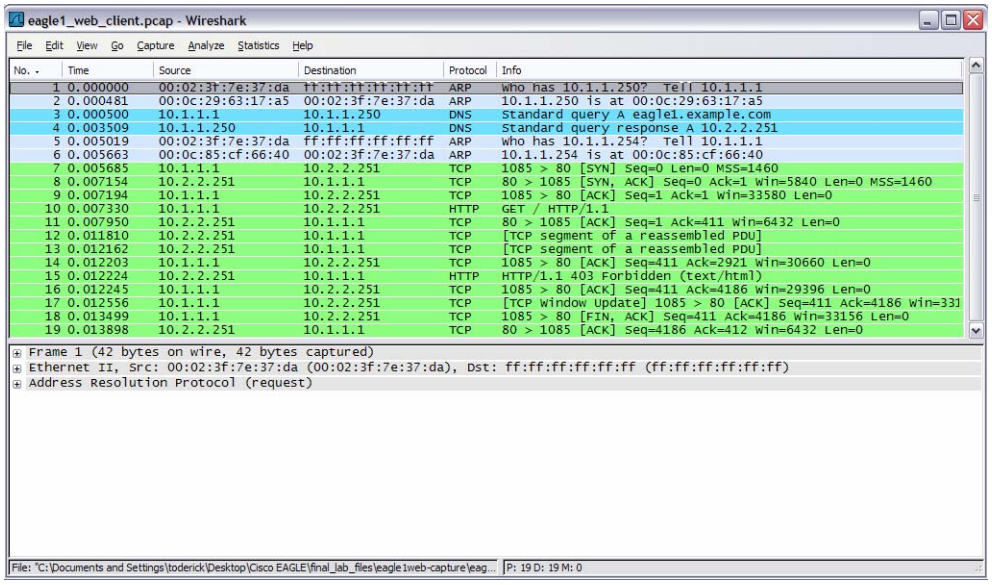

图 5. 已加载 eagle1_web_client.pcap 文件的 Wireshark 窗口。

任务 2：回顾数据流经网络的过程。

步骤 1：回顾传输层的运作。

当 PC_Client 创建用于连接 eagle1.example.com 的数据报时，该数据报会途经各个网络层。每层都会向该数据报加入重要的报头信息。因为此通信是从 web 客户端发起，因此传输层协议将为 TCP。如图 6 所示，考虑 TCP 数据段。PC_Client 生成一个内部 TCP 端口地址（在本会话中为 1085），而且知道公认的 web 服务器端口地址为 80。当然，还会从内部生成一个序列号。数据由应用层打包并提供。PC_Client 尚不清楚某些信息，因此必须使用其他网络协议来发现。

无确认号。必须进行 TCP 三次握手，此数据段才能移到网络层。

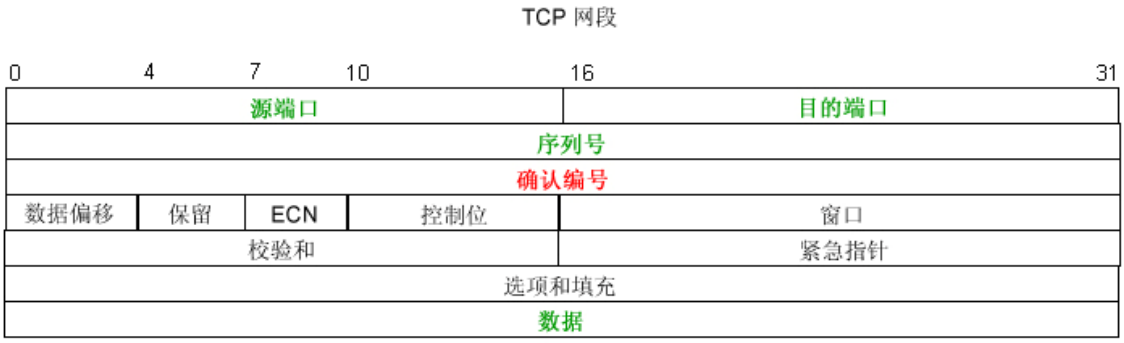

图 6. TCP 数据段的各个字段。

步骤 2：回顾网络层的运作。

在网络层，IPv4 (IP) 数据包的好几个字段中的信息已备妥。如图 7 所示，例如，数据包版本 (IPv4) 和源 IP 地址均为已知。

此数据包的目的地为 eagle1.example.com，相应的 IP 地址必须通过 DNS（域名服务）来发现。在收到上层数据报之前，与上层协议相关的字段都保持空白。

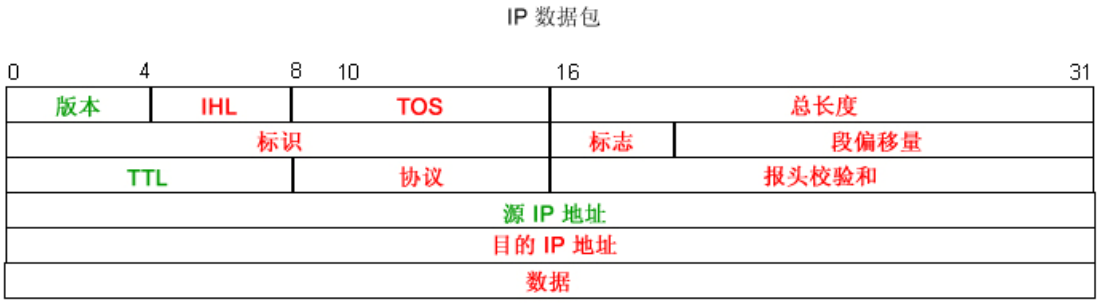

图 7. IP 数据包的各个字段。

步骤 3：回顾数据链路层的运作。

数据报必须封装在帧内才能放到物理介质上。此情景如图 8 所示，PC_Client 知道源 MAC 地址，但必须发现目标 MAC 地址。

必须发现目标 MAC 地址。

以太网 II 帧格式

前导码	目的地址	源地址	帧类型	数据	CRC
8 个八位字节	6 个八位字节	6 个八位字节	2 个八位字节	46-1500 个八位字节	4 个八位字节

图 8. Ethernet II 帧的各个字段。

任务 3：分析捕获的数据包。

步骤 1：回顾数据流序列。

回顾缺失的信息有助于追踪捕获的数据包序列：

a. 无法构建 TCP 数据段，原因在于确认字段仍空白，必须与 eagle1.example.com 完成一次 TCP 三次握手。

b. 无法进行 TCP 三次握手，原因在于 PC_Client 不知道 eagle1.example.com 的 IP 地址，解决方法是从 PC_Client 向 DNS 服务器发送一个 DNS 请求。

c. 无法查询 DNS 服务器，原因在于不知道 DNS 服务器的 MAC 地址。因此，将向 LAN 广播 ARP 协议以发现 DNS 服务器的 MAC 地址。

d. 不知道 eagle1.example.com 的 MAC 地址。因此将向 LAN 广播 ARP 协议以获取 eagle1.example.com 的目标 MAC 地址。

步骤 2：研究 ARP 请求。

请参阅 Wireshark 的数据包列表窗口中的第 1 号数据包，捕获的帧是一个 ARP（地址解析协议）请求。单击数据包详细信息窗口中第二行的复选框，即可查看该 Ethernet II 帧的内容。单击数据包详细信息窗口中的 ARP 请求行，即可查看该 ARP 请求的内容。

1. 该 ARP 请求的源 MAC 地址是什么？_____

2. 该 ARP 请求的目标 MAC 地址是什么？_____

3. 该 ARP 请求中的未知 IP 地址是什么？_____

4. 该 Ethernet II 帧的类型是什么？_____

步骤 3：研究 ARP 回应。

请参阅 Wireshark 的数据包列表窗口中的第 2 号数据包，DNS 服务器发送了一个 ARP 回应。

1. 该 ARP 回应的源 MAC 地址是什么？_____
2. 该 ARP 请求的目标 MAC 地址是什么？_____
3. 该 Ethernet II 帧的类型是什么？_____
4. 该 ARP 回应中的目标 IP 地址是什么？_____
5. 根据对 ARP 协议的观察，可以对 ARP 请求的目标地址以及 ARP 回应的目标地址作出怎样的推断？
   _____
   _____
   _____
6. 为什么 DNS 服务器不必发送 ARP 请求以获取 PC_Client 的 MAC 地址？
   _____
   _____

步骤 4：研究 DNS 查询。

请参阅 Wireshark 的数据包列表窗口中的第 3 号数据包，PC_Client 向 DNS 服务器发送了一个 DNS 查询。使用数据包详细信息窗口回答下列问题：

1. 该 Ethernet II 帧的类型是什么？_____
2. 该传输层协议是什么？目标端口号是多少？_____

步骤 5：研究 DNS 查询回应。

请参阅 Wireshark 的数据包列表窗口中的第 4 号数据包，DNS 服务器向 PC_Client 发送了一个 DNS 查询回应。使用数据包详细信息窗口回答下列问题：

1. 该 Ethernet II 帧的类型是什么？_____
2. 该传输层协议是什么？目标端口号是多少？_____
3. eagle1.example.com 的 IP 地址是什么？_____
4. 有个同事是防火墙管理员，他问您是否考虑过为什么不能阻挡所有 UDP 数据包进入内部网络。您会怎样回答？_____
   _____
   _____
   _____

步骤 6：研究 ARP 请求。

请参阅 Wireshark 的数据包列表窗口中的第 5 和第 6 号数据包，PC_Client 向 IP 地址 10.1.1.254 发送了一个 ARP 请求。

1. 此 IP 地址和 eagle1.example.com 的 IP 地址不同吗？如何解释？

   _____
   _____

步骤 7：研究 TCP 三次握手。

请参阅 Wireshark 的数据包列表窗口中的第 7、第 8 和第 9 号数据包，这些数据包包含 PC_Client 与 eagle1.example.com 之间的三次握手信息。起初，从 PC_Client 发出的数据报中仅设置了 TCP SYN 标志，序列号为 0。在 eagle1.example.com 发出的回应中，已设置了 TCP ACK 标志和 SYN 标志，确认号为 1 且序列号为 0。在数据包列表窗口中，有一个未解释的值 **MSS=1460**。MSS 代表最大数据段大小。当通过 IPv4 传输 TCP 数据段时，MSS 通过最大 IPv4 数据报大小减去 40 字节算得。此值在连接启动时发送。与此同时，会协商 TCP 滑动窗口。

1. 如果来自 PC_Client 的初始 TCP 序列值为 0，为什么 eagle1.example 回应的确认号为 1 呢？

   _____
   _____

2. 在 eagle1.example.com 中，第 8 号数据包中的 IP 标志值 0x04 有何含义？

   _____

3. 请参阅 Wireshark 数据包列表中的第 9 号数据包，当 PC_Client 完成三次握手时，返回 eagle1.example.com 的 TCP 标志状态是怎样的？

   _____

任务 4：完成最终分析。

步骤 1：将 Wireshark 输出与过程匹配。

当在 PC_Client、DNS 服务器、网关以及 eagle1.example.com 之间发送了共九个数据报后，PC_Client 才获得了足够信息，可以向 eagle1.example.com 发送原始的 web 客户端请求了。请参阅 Wireshark 数据包列表中的第 10 号数据包，PC_Client 发送了一个 web 协议 GET 请求。

1. 填入符合下列缺失条目的正确 Wireshark 数据包列表编号：

   a. 无法构建 TCP 数据段，原因在于确认字段仍空白，必须与 eagle1.example.com 完成一次 TCP 三次握手。_____

   b. 无法进行 TCP 三次握手，原因在于 PC_Client 不知道 eagle1.example.com 的 IP 地址，解决方法是从 PC_Client 向 DNS 服务器发送一个 DNS 请求。_____

c. 无法查询 DNS 服务器，原因在于不知道 DNS 服务器的 MAC 地址。因此，将向 LAN 广播 ARP 协议以发现 DNS 服务器的 MAC 地址。_____

d. 不知道通向 eagle1.example.com 的网关的 MAC 地址。因此将向 LAN 广播 ARP 协议以获取网关的目标 MAC 地址。_____

2. Wireshark 数据包列表中的第 11 号数据包是 eagle1.example.com 对 PC_Client 发出的 GET 请求（Wireshark 数据包列表中的第 10 号数据包）的确认。

3. Wireshark 数据包列表中的第 12、13 和 15 号数据包是来自 eagle1.example.com 的 TCP 数据段，第 14 和 16 号数据包则是来自 PC_Client 的 ACK 数据报。

4. 要验证 ACK，请突出显示 Wireshark 数据包列表中的第 14 号数据包，然后滚动到详细信息列表窗口底部，并展开 [SEQ/ACK analysis]（SEQ/ACK 分析）帧。Wireshark 数据包列表中的第 14 号数据包中的 ACK 数据报用于回应来自 eagle1.example.com 的哪个数据报？

   _____

5. Wireshark 数据包列表中的第 17 号数据报由 PC_Client 发往 eagle1.example.com。回顾 [SEQ/ACK analysis]（SEQ/ACK 分析）帧中的信息。此数据报的用途是什么？

6. 当 PC_Client 完成时，发出 TCP ACK 标志和 FIN 标志，此情景如 Wireshark 数据包列表中的第 18 号数据包所示。eagle1.example.com 使用一个 TCP ACK 回应，该 TCP 会话至此关闭。

步骤 2：Use Wireshark TCP 数据流。

分析数据包内容是一项困难、费时且容易出错的体验。Wireshark 提供了一个选项，它可用于在另一个窗口中构建 TCP 数据流。要使用此功能，首先，请从 Wireshark 数据包列表中选择一个 TCP 数据报。接下来，选择 Wireshark 菜单选项 Analyze（分析）| Follow TCP Stream（追踪 TCP 数据流）。将出现类似图 9 的窗口。

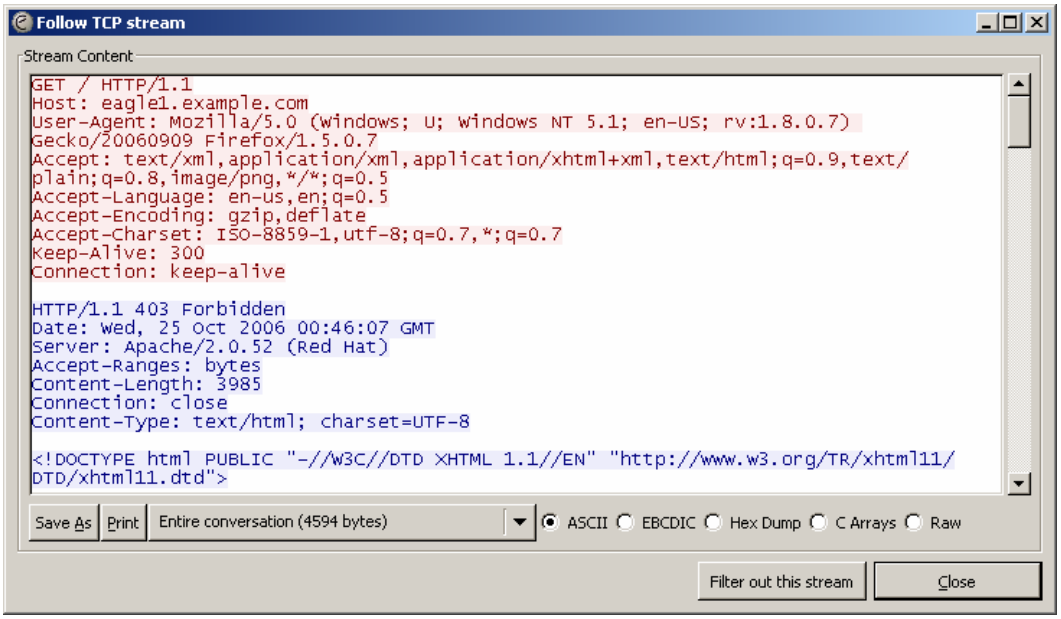

图 9. TCP 数据流的输出。

任务 5：结论

网络协议分析程序可用作理解网络通信要素的有效学习工具。一旦网络管理员熟悉了通信协议，该网络协议分析程序就变成了网络管理员手中排除网络故障的利器。例如，如果一个 web 浏览器无法连接到 web 服务器，原因可能有很多种。协议分析程序可显示未成功的 ARP 请求、未成功的 DNS 查询和未获确认的数据包。

任务 6：总结

在本练习中，学生学习了 web 客户端与 web 服务器之间的通信过程。诸如 DNS 和 ARP 之类的幕后协议用于填充 IP 数据包和以太网帧的缺失部分。必须通过 TCP 三次握手构建可靠的路径并为通信双方提供初始 TCP 报头信息，才能开始 TCP 会话。最后，随着客户端发出 TCP FIN 标志，TCP 会话被井然有序地关闭。