实验 3 分析 Ethernet II 帧、分析集线器和交换机工作机理

第一部分 分析 Ethernet II 帧

1. 实验目的

1)深入理解 Ethernet II 帧结构。
2)基本掌握使用 Wireshark 分析俘获的踪迹文件的基本技能。

2. 实验环境

1)运行 Windows 2008 Server/Windows XP/Windows 7 操作系统的 PC 一台。
2)PC 具有以太网卡一块，通过双绞线与网络相连；或者具有适合的踪迹文件。
3)每台 PC 运行程序协议分析仪 Wireshark。

3. 实验步骤

1)分析踪迹文件中的帧结构

用 Wireshark 俘获网络上收发分组或者打开踪迹文件，选取感兴趣的帧进行分析。如图 18 所示，选取第 10 号帧进行分析。在首部细节信息栏中，可以看到有关该帧的到达时间、帧编号、帧长度、帧中协议和着色方案等信息。在“帧中协议”中，看到该帧有“Ethernet:IP:ICMP:data”的封装结构。

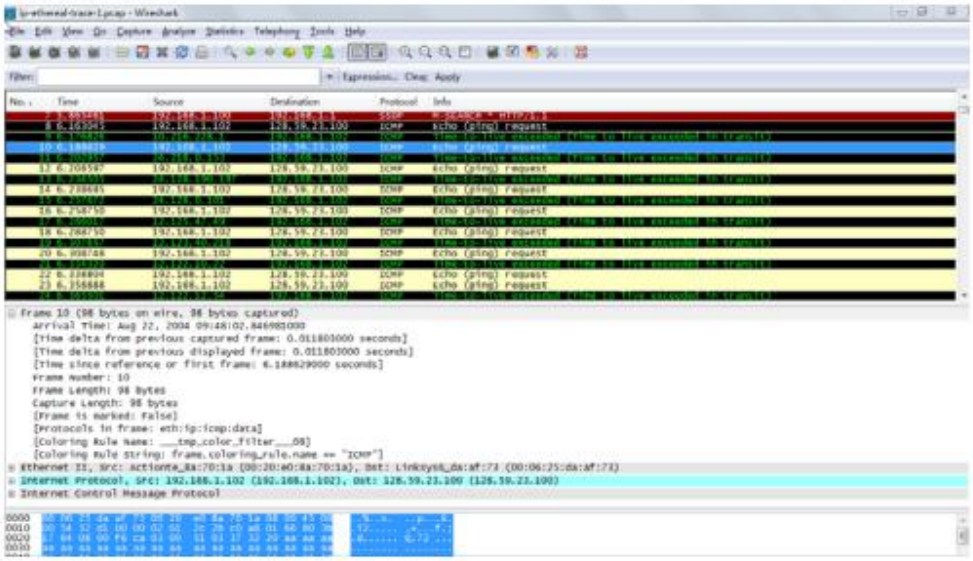

图 18 分析帧的基本信息

为了进一步分析 Ethernet II 帧结构，点击首部细节信息栏中的“Ethernet II”行，有关信息展开如图 19 所示。

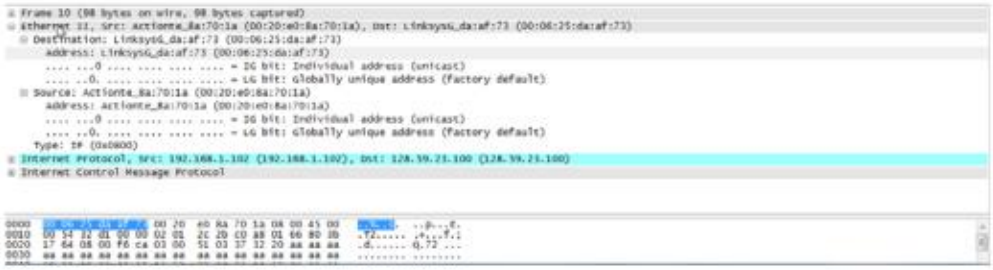

图 19　Ethernet II 帧详细信息

其中看到源 MAC 地址为 00:20:e0:8a:70:1a，目的 MAC 地址为 00:06:25:da:af:73；以太类型字段中值为 0x0800，表示该帧封装了 IP 数据报；以及 MAC 地址分配的相关信息。

2)分析以太帧结构

将计算机联入网络，打开 Wireshark 俘获分组，从本机向选定的 Web 服务器发送 Ping 报文。回答下列问题：

(1) 本机的 48 比特以太网 MAC 地址是什么？

(2) 以太帧中目的 MAC 地址是什么？它是你选定的远地 Web 服务器的 MAC 地址吗？(提示：不是)那么，该地址是什么设备的 MAC 地址呢？(这是一个经常会误解的问题，希望搞明白。)

(3) 给出 2 字节以太类型字段的十六进制的值。它表示该以太帧包含了什么样的协议？上网查找如果其中封装的 IPv6 协议，其值应为多少？

4. 相关概念

1) IEEE 802.3 以太帧结构。它是在以太网链路上运行的一种数据分组，开始于前导码和帧定界符起始，后继的是以太首部的目的和源地址。该帧的中部是载荷数据，其中包括了由该帧携带的其他协议(如 IP)的首部。该帧的尾部是 32 比特的循环冗余码校验，以检测数据传输时可能的损伤。它完整的帧结构如图 20 所示。

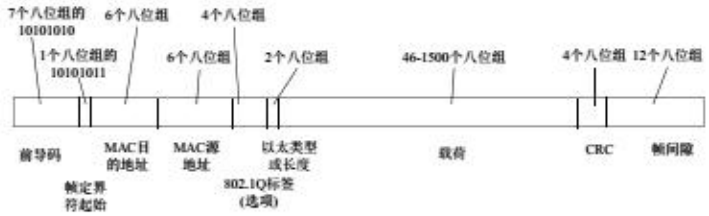

图 20　802.3 以太帧结构

2) Ethernet II 帧结构。有几种不同类型的帧结构，尽管它们格式和最大传输单元不同，但却能够共存于相同的物理媒体上。Ethernet II 帧(又称 DIX 帧)是目前使用最广的以太帧。图 21 显示了 Ethernet II 帧结构(该帧前后的辅助字段没有显示)。与 802.3 以太帧结构相比，它较为简单。其中的以太类型字段标识了封装了该帧数据中的较高层协议。例如，以太类型值为 0x0800 指示了该帧包含了 IPv4 数据报，0x0806 表明指示了该帧包含了 ARP 帧，0x8100 指示了该帧包含了 IEEE 802.1Q 帧。

图 21　802.3 以太帧结构

第二部分 分析集线器和交换机工作机理

1. 实验目的

1)观察交换机处理广播和单播报文的过程。

2)比较交换机与集线器工作过程。

3)掌握使用 PacketTracer 模拟网络场景的基本方法，加深对网络环境、网络设备和网络协议交互过程等方面的理解。

2. 实验环境

1)运行 Windows 2008 Server/Windows XP/Windows 7 操作系统的 PC 一台。
2)下载 CISCO 公司提供的 PacketTracer 版本 5.2.1。

3. 实验步骤

1)在 PacketTracer 模拟器中配置网络拓扑

在 PacketTracer 模拟器中配置如图 22 所示的网络拓扑，其中通用交换机连接 4 台普通 PC，通用集线器 hub 连接 2 台普通 PC。

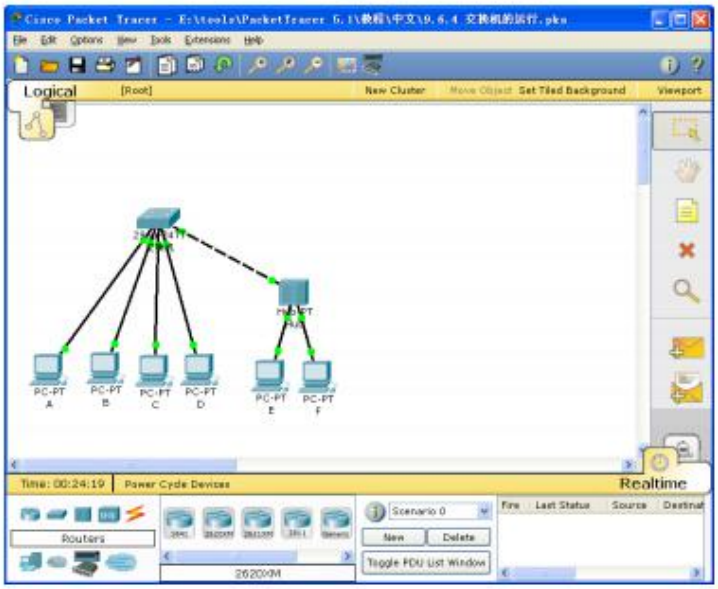

图 22　实验网络拓扑图

点击 PC，在每台 PC 的配置窗口中配置合理的 IP 地址和子网掩码，无需为交换机和集线器配置 IP 地址(为什么？)。

2)观察交换机如何处理广播和单播报文

(1) 在实时与模拟模式之间切换 4 次，完成生成树协议。所有链路指示灯应变为绿色。最后停留在模拟模式中。

(2) 使用 Inspect(检查)工具(放大镜)打开 PC A 和 PC B 的 ARP 表以及交换机的 MAC 表。本练习不关注交换机的 ARP 表。将选择箭头移到交换机上，查看交换机端口及其接口 MAC 地址的摘要。注意，这不是交换机获取的地址表。将窗口排列在拓扑上方。

(3) 添加简单 PDU 以从 PC A 发送 ping 到 PC B(也可以在 PC A 的 DeskTop 窗口中打开模拟命令行“Command Prompt”，运行 PING 命令)。

使用 Add Simple PDU(添加简单 PDU)(闭合的信封)从 PC A 发送一个 ping 到 PC B。点击 PC A(源)，然后点击 PC B(目的)。Event List(事件列表)中将会显示两个事件：一个 ICMP 回应请求和一个 ARP 请求，用以获取 PC B 的 MAC 地址。点击 Info(信息)列中的彩色框以检查这些事件。

(4) 逐步运行模拟。

使用 Capture/Forward(捕获/转发)按钮跟踪数据包的最终顺序。由于 PC A ARP 表中没有 PC B 的相应条目，因此为了完成 ping，它必须发出 ARP 请求。交换机从 ARP 请求获取 PC A 的 MAC 地址及其连接的端口，从 ARP 回复获取 PC B 的 MAC 地址及其连

接的端口，交换机会将 ARP 请求从所有端口泛洪出去，因为 ARP 请求始终是广播。PC A 收到 ARP 回复之后，便可以完成 ping。从交换机的角度来看，ping 是已知单播。完成对数据包的跟踪之后，点击 Reset Simulation(重置模拟)按钮。

3)观察交换机如何处理未知单播(可选)

(1) 清除交换机的 MAC 地址表。

点击交换机。点击 CLI 选项卡。在出现命令提示符时，按几次 Enter 键，将会显示 Switch> 提示。键入 enable 并按 Enter 键。提示应会变为 Switch#。键入命令 clear mac-address-table dynamic 并按 Enter 键。请注意，早先显示的交换机 MAC 表重新为空。但仍会填充 PC ARP 表。关闭交换机配置窗口。

(2) 重新发送数据包。

您应该还是处于模拟模式。用户创建的 PDU(在任务 1 中创建的从 PC A 到 PC B 的 ping)仍然在 Event List(事件列表)中。使用 Capture/Forward(捕获/转发)按钮跟踪数据包的最终顺序。由于 ARP 表已经填充，因此无需 ARP 请求。但是，当回应请求数据包到达 MAC 地址表为空的交换机时，将被视为未知单播。在这种情况下，交换机就会像处理广播一样，将数据包从除接收端口以外的所有其他端口泛洪出去。完成之后，点击 Delete(删除)按钮删除场景 0。

4)观察交换机和集线器的工作过程

(1) 现在尝试使用 Add Simple PDU(添加简单 PDU)按钮从 PC E ping PC A。跟踪数据包，尝试了解发生的变化。

(2) 进行其他实验，了解交换机和集线器的不同。

4. 相关概念

集线器工作在物理层，仅对电信号进行放大整形向所有端口转发，并不识别数据链路层的帧，更不执行 CSMA/CD 协议。

交换机工作在数据链路层，对接口接收的数据链路层的帧进行处理，查看其目的 MAC 地址，选择正确的接口进行存储转发，在向其他接口转发时要执行 CSMA/CD 协议。交换机通过其接收的帧来学习每个端口连接的设备的物理地址，并将该信息存储在地址表中。如果交换机收到的帧的目的设备物理地址在其地址表中，它只会将该帧从连接该设备的端

口发送出去。这称为已知单播。如果交换机收到一个广播，就会将该帧从接收端口以外的所有其他端口泛洪出去。另外，如果交换机收到的帧的目的设备 MAC 地址不在其地址表中(即未知单播)，它也会将该帧从除接收端口以外的所有其他端口泛洪出去。当交换机将帧从除接收端口以外的所有其他端口泛洪出去时，其行为类似于集线器。

一个集线器形成了一个网络碰撞域；而对局域网交换机而言，每个端口可能构成一个独立的碰撞域，大大减少了分组访问网络冲突的机会。只要 PC 两两之间访问交换机的不同端口，并且这些端口配置为全双工的，它们之间就不存在碰撞域。广播域是对广播分组直接到达的区域而言的，由于局域网交换机转发广播报文，因此由交换机连接的局域网构成了一个广播域。

5. 注意事项

PacketTracer 功能很强大，用户可以自行设计各种网络拓扑，验证学习过的网络原理。