# 实验 4 分析 IP 和 ARP 协议

## 一、分析 IP

### 1. 实验目的

1)深入理解 IP 报文结构和工作原理。
2)掌握用 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，通过双绞线与校园网相连；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)分析俘获的分组

打开踪迹文件，用鼠标点选感兴趣的帧，按右键出现如图 23 菜单。该菜单提供了许多非常有用的功能，详细情况可以参见系统软件自带的“Wireshark 用户指南”的表 6.1。例如，当选中编号 10 的分组，用鼠标指向其源地址，打开如图 23 所示菜单，点击“Selected”，就会出现如图 24 所示的界面。可见，系统已经自动用其源地址作为过滤条件，从众多分组中过滤出与 192.168.1.100 有关分组了。更一般的定义过滤条件，可以选用“Analyze/Display Filters”功能。有关过滤条件的表示，可以参见“Wireshark 用户指南”6.4 节的内容。

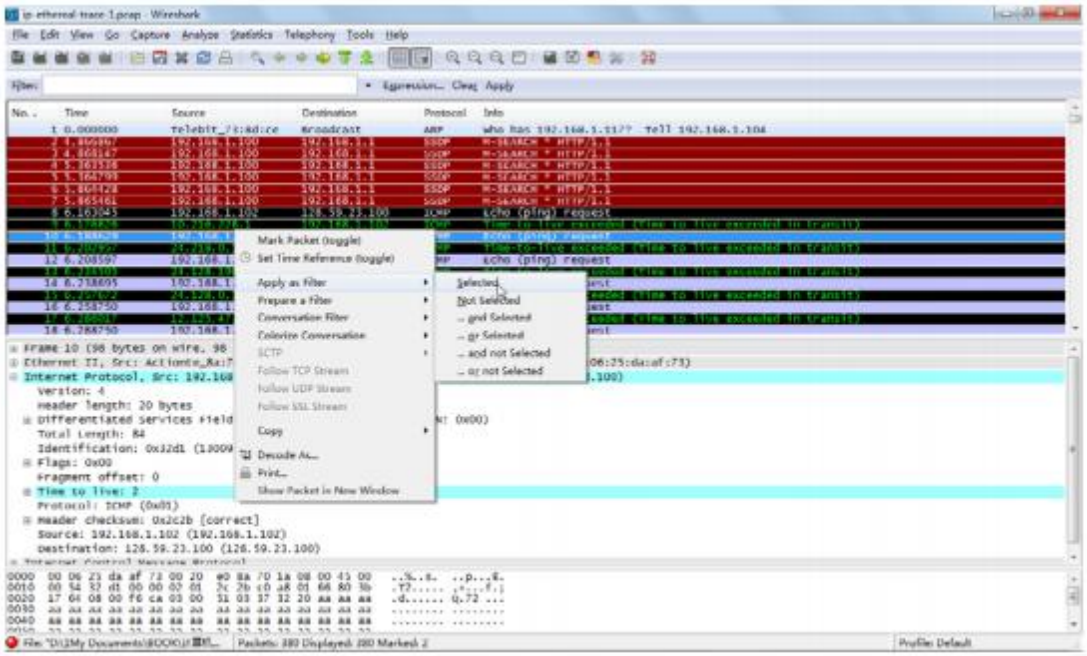

图 23 分组列表窗口的弹出菜单

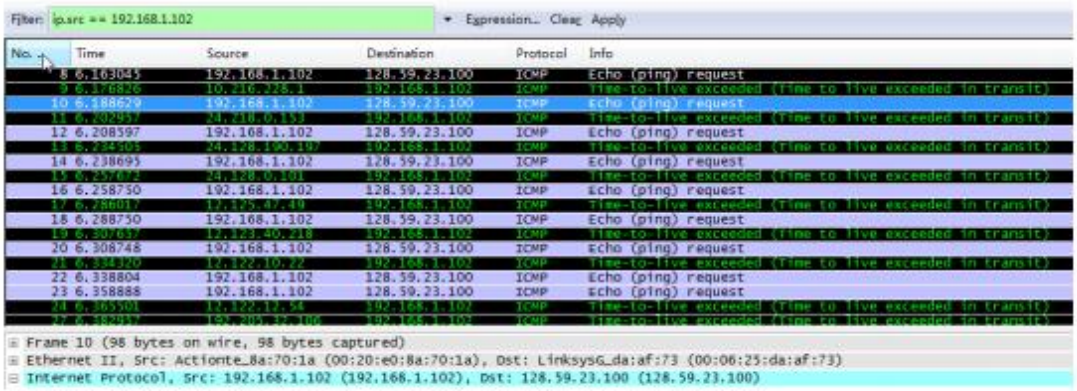


图 24 以源地址作为条件进行过滤

有时为了清晰起见，需要屏蔽掉较高层协议的细节，可以点击“Analyze/Enable Protocols”打开“Profile: Default”窗口，若去除选择 IP，则将屏蔽 IP 相关的信息。

**2)分析 IP 报文结构**

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。选中其中一条 Ping 报文，该帧中的协议结构是：Ethernet: IP: ICMP: data。为了进一步分析 IP 数据报结构，点击首部细节信息栏中的“Internet Protocol”行，有关信息展开如图 25 首部信息窗口所示。

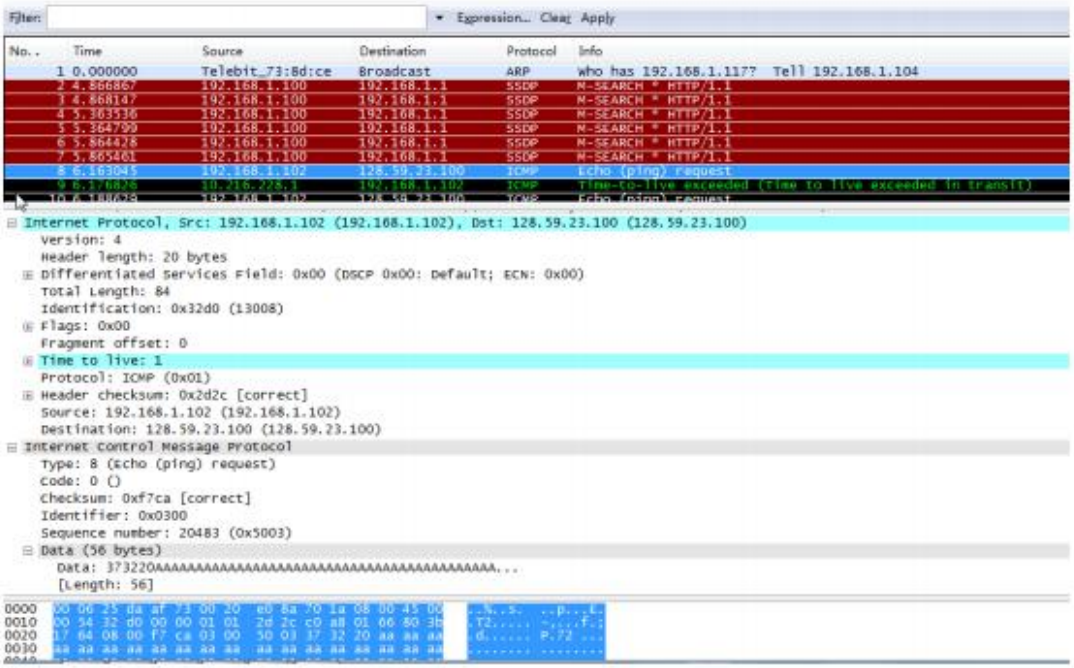


图 25 “Internet Protocol”详细信息

回答下列问题：

(1) 你使用的计算机的 IP 地址是什么？

(2) 在 IP 数据报首部，较高层协议字段中的值是什么？

(3) IP 首部有多少字节？载荷字段有多少字节？

(4) 该 IP 数据报分段了没有？如何判断该 IP 数据报有没有分段？

(5) 关于高层协议有哪些有用信息？

**4. 相关概念**

1)网际协议(Internet Protocol，IP)数据报格式。它是 TCP/IP 体系中两个最主要的协议之一，也是最重要的因特网标准协议 [RFC 791] 之一。图 26 显示了 IP 数据报的格式。


图 20 IP 数据报格式

2)互联网控制报文协议报文格式。互联网控制报文协议(Internet Control Message Protocol，ICMP)由[RFC 792]定义，它用于主机路由器彼此交互网络层信息。ICMP 最典型

的用途是差错报告。图 27 为 ICMP 的报文格式。

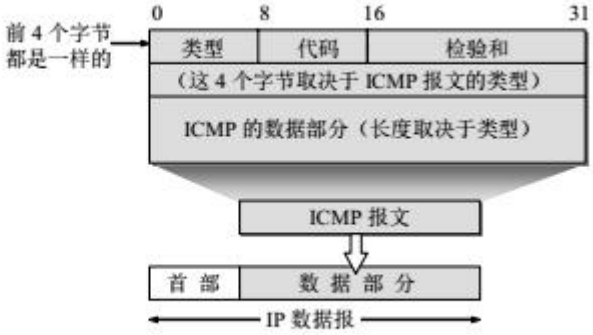


图 27　ICMP 报文格式

## 二、分析 ARP 协议

### 1. 实验目的

1)深入理解地址解析协议(ARP)的工作原理。

2)理解 IP 和以太网协议的关系，掌握 IP 地址和 MAC 地址的映射机制，搞清楚 IP 报文是如何利用底层的以太网帧进行传输的。

### 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)查看本机因特网硬件地址

ipconfig 是 Windows 操作系统中调试网络配置的常用命令，其主要功能包括显示主机的网络配置信息(通过/all 参数)、释放获得的 IP 地址信息(通过/release 参数)，或者重新获取 ip 地址信息(通过/renew 参数)等。本次实验主要学习使用 ipconfig 查看计算机网卡的物理地址，对其他功能感兴趣的读者可以通过 ipconfig /?命令查看相应的使用帮助。

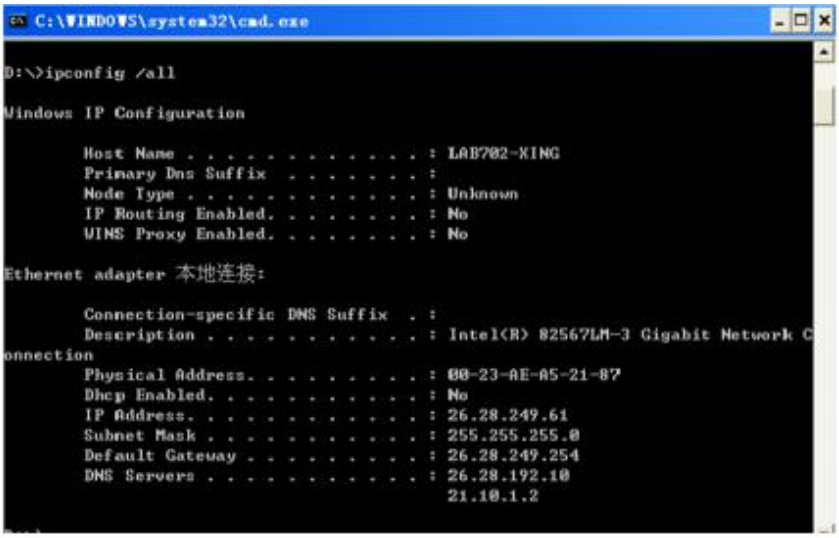


图 31 ipconfig 基本命令

在“运行”窗口中输入“cmd”后，在打开的“命令提示符”窗口中输入“ipconfig /all ”命令，可以看到类似于图 31 所示的有关网络连接的信息。其中，主机的名字为 LAB702-XING，以太网络适配器为 Intel(R) 82567LM-3 Gigabit Network Connection，其 MAC 地址为 00-23-AE-A5-21-87，DHCP 功能关闭，IP 地址为 26.28.249.61，掩码为 255.255.255.0，默认网关是 26.28.249.254，DNS 服务器是 26.28.192.10 和 21.10.1.2。

**2)使用 ARP 命令**

通过 ARP 命令能够显示和修改 ARP 高速缓存中 IP 地址和 MAC 地址的映射表，与 ipconfig 类似，该命令同样包含多种参数，可以首先在“命令提示符”界面中输入“arp /?”查看 ARP 命令的使用帮助，如图 32 所示。

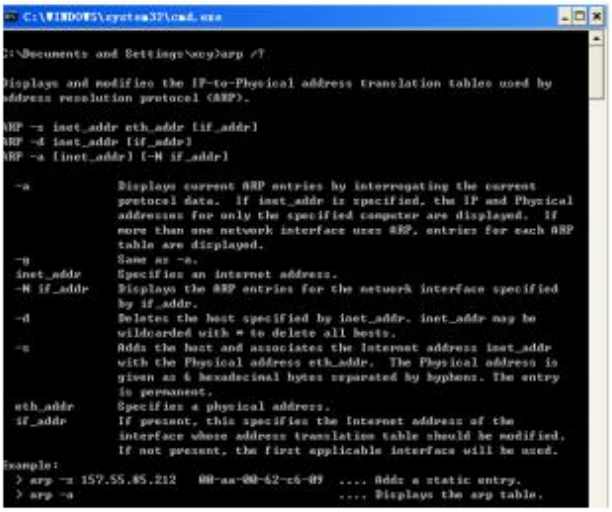


图 32 ARP 帮助信息

由图 32 可以看到，ARP 命令主要功能包括显示当前 ARP 高速缓存中全部的 IP 地址和 MAC 地址映射信息、删除当前 ARP 高速缓存中的地址映射信息、以及增加一条静态地址映

射信息等，下面分别对这 3 个主要功能加以说明。

在“命令提示符”界面中键入“arp –a”指令，可以查看本机 ARP 表中的全部内容，如图 33 所示。可以看到，在 ARP 高速缓存表中每个表项包括 3 个部分：主机 IP 地址，主机物理地址以及表项类型，其中表项类型中 dynamic 表明该表项状态为动态更新，一段时间未刷新将会被删除，static 表明该表项为静态绑定，除非主动删除该表项将一直存在。

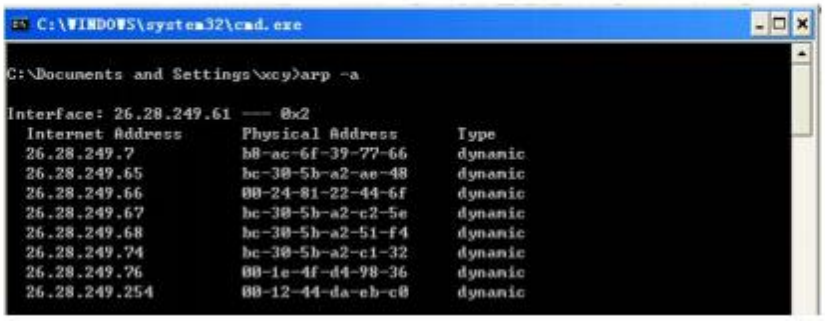


图 33 查看本机 ARP 缓存表中信息

“arp –d”命令用于主动清除 ARP 表中的全部记录，如图 34 所示，执行过“arp –d”命令后，再次执行“arp –a”命令可以发现系统提示不存在 ARP 表项。

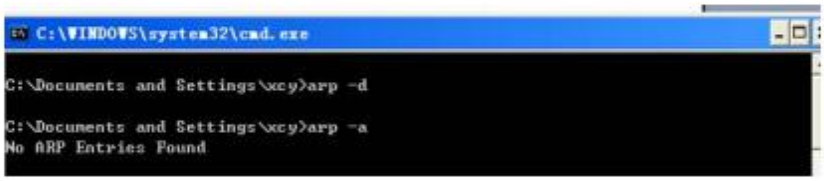


图 34 主动清空 ARP 表项

如果仅希望删除 ARP 表中的部分表项，可以在“arp –d”命令后加相应的 IP 地址参数，例如“arp –d 26.28.249.254”将仅删除 ARP 表中 IP 地址为 26.28.249.254 的表项。

“arp –s”命令允许人们手工在 ARP 表项中增加一条 IP 地址和物理地址的绑定记录，其命令格式为“arp –s 26.28.249.1 00-12-36-fe-eb-dc”，如图 35 所示，执行该命令后，在 ARP 表中增加了一条表项，并且其类型字段为 static，表明是一个静态绑定的表项。

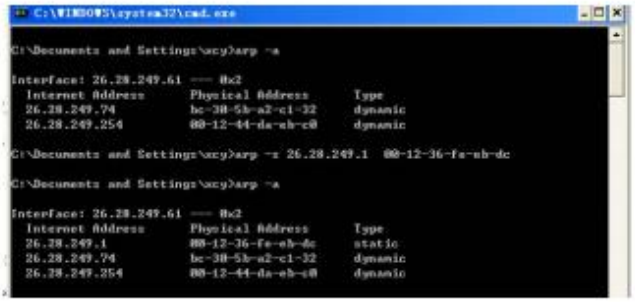


图 35 手工添加一条静态 ARP 表项

**3)分析 ARP 协议工作过程**

(1) 在实验室中选择两台相连的计算机，清除 ARP 表中的所有项目。

本次实验选择 IP 地址为 26.28.249.61 的主机 A 和 26.28.249.74 的主机 B 进行实验，首

先在主机 A 与 B 上分别执行“arp –d”命令清除 ARP 表中的所有项目，如图 36 所示。


图 36 清空主机 ARP 表项

(2) 在主机 A 上运行 Wireshark 程序，执行包俘获操作。

(3) 从主机 A 向主机 B 发送 Ping 包，稍后停止发 Ping 包。分别检查两台主机的 ARP 表中项目。

如图 37 所示，可以发现此时主机 A 的 ARP 表项中增加了一条关于主机 B 的表项，检查主机 B 的 ARP 表可以发现类似结论。


图 37 查看主机 ARP 表项

(4) 从俘获的分组中找出 ARP 报文，并分析 ARP 协议执行的全过程，画出或写出 ARP 协议报文的交互过程，分析实验结果和现象。

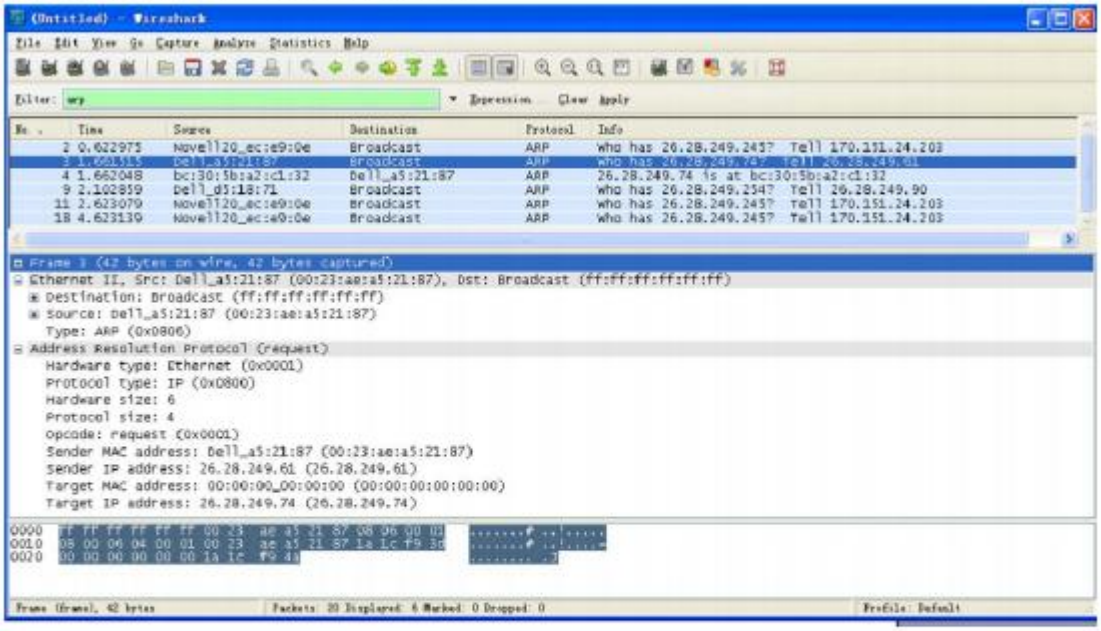


图 38 ARP 请求报文分析

图 38 显示了本次通信过程的分组俘获情况，并且为了清晰起见，运用 arp 作为过滤器，以便只显示通信过程中的 ARP 报文，分析发现报文 2 为主机 A 发送的 ARP 请求报文，进一步分析其报文结构可以发现，ARP 报文是封装在以太帧中传输，并且在以太帧中协议类型为 0x0806，其源 MAC 地址为主机 A 的 MAC 地址 00:23:ae:a5:21:87，目的 MAC 地址为

广播地址 ff:ff:ff:ff:ff:ff，表明 ARP 请求报文是一个广播帧。ARP 协议中硬件类型为以太网，协议类型为 IP，硬件地址和协议地址的长度分别为 6 字节(48 bits MAC 地址)和 4 字节(32 bits IP 地址)，操作类型为 ARP 请求报文(0x0001)，发送方的 MAC 地址和 IP 地址分别为 00:23:ae:a5:21:87 和 26.28.249.61，目标方的 MAC 地址未知(全 0 填充)，IP 地址为 26.28.249.74。

报文 4 为主机 B 向主机 A 发送的 ARP 应答报文，图 39 给出了其详细结构，可见其同样是封装在以太帧中传输，但源 MAC 地址为主机 B 的 MAC 地址 bc:30:5b:a2:c1:32，目的 MAC 地址为主机 A 的 MAC 地址 00:23:ae:a5:21:87(思考为什么不像 ARP 请求报文那样设为广播地址？)。ARP 操作类型为 ARP 应答报文(0x0002)，发送方的 MAC 地址和 IP 地址分别为 bc:30:5b:a2:c1:32 和 26.28.249.74，目标方的 MAC 地址为 00:23:ae:a5:21:87，IP 地址为 26.28.249.61。

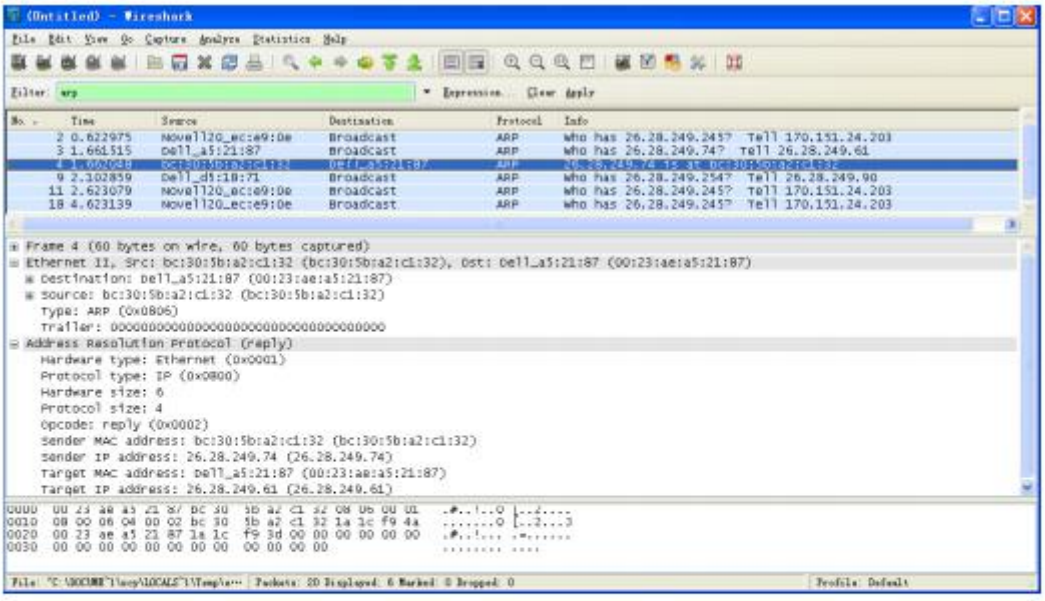


图 39　ARP 应答报文分析

完成上述交互过程后，通信双方均已获得彼此的 MAC 地址，随后即可以进行正常通信。

思考：在本次通信过程中，为何只有主机 A 到主机 B 的 ARP 请求？主机 B 是如何获得主机 A 的 MAC 地址的？

**4. 相关概念**

每一个主机都设有一个 ARP 高速缓存(ARP cache)，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表，这些都是该主机目前知道的一些地址。例如，当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。如有，就可以查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网把该 MAC 帧发往此硬件地址。若查不到主机 B 的 IP 地址的项目，主机 A

就自动运行 ARP，向所在局域网广播一个 ARP 查询，查询主机 B 的硬件地址，该查询中包含主机 B 的 IP 地址。主机 B 在应答中包含其硬件地址，主机 A 将 B 的硬件地址添加到其 ARP 缓存中供以后使用。

**5. 注意事项**

1) 除本次实验用到的功能外，ipconfig 命令与 arp 命令均还有一些强大功能，读者可以参阅两条命令的帮助文件学习其他功能的用法。

2) 当网络规模较大时，Wireshark 会俘获很多与本实验无关的通信分组，可以在过滤器中设置相应过滤条件以便于分析。