ARP

一 实验目的

1. 理解 ARP 协议的作用
2. 掌握 ARP 协议的报文格式
3. 理解 ARP 协议的工作原理
4. 了解 ARP 协议的高速缓存

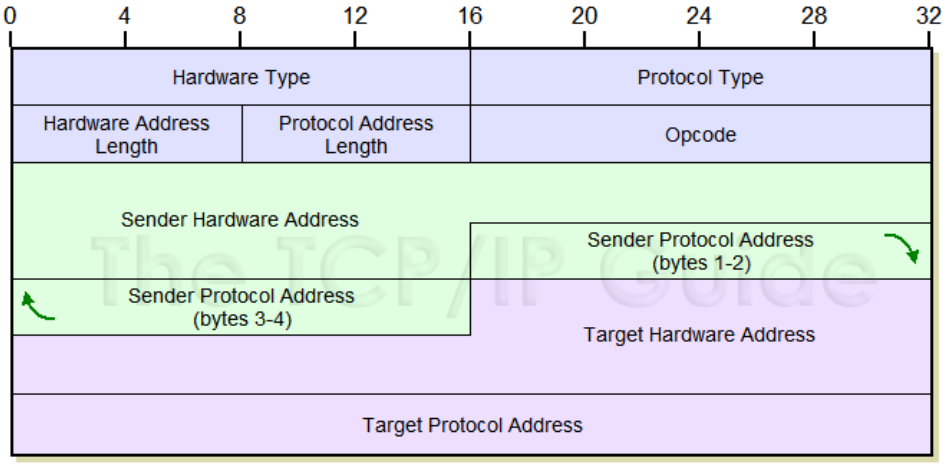
二 预备知识

1. MAC 地址

我们知道在网络中通讯，都是知道对方的 IP 地址后，才能发起连接，IP 地址所在的层是网络层，而在网络层下面是数据链路层，这里 IP 数据包继续被封装成以太网数据帧，当然还有别的数据链路层格式，但是数据链路层也需要寻址机制，常常就是 48bit 的硬件地址,又叫 MAC 地址。MAC 地址就是在媒体接入层上使用的地址，也叫硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。MAC 地址与网络无关，也即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，都有相同的 MAC 地址，它由厂商写在网卡的 BIOS 里。

2. ARP 协议

ARP(Address Resolution Protocol)即地址解析协议，用于实现从 IP 地址到 MAC 地址的映射，即询问目标 IP 对应的 MAC 地址。一般情况下，上层应用程序更多关心 IP 地址而不关心 MAC 地址，所以需要通过 ARP 协议来获知目的主机的 MAC 地址，完成数据封装。ARP 报文长度为 28 字节，格式如下：



ARP 报文中各字段含义为:

1. Hardware Type：占 2 个字节，表示传输 ARP 报文的物理网络类型，最常见的是以太网类型，对应的值是 1。
2. Protocol Type：协议类型，字段长度是 2 字节。最常用的是 IPv4 报文，对应的值是 2048（十六进制为 0x0800，这和以太网帧中帧类型字段使用的 IP 报文类型字段的值相同）。

3. Hardware Address Length：物理地址长度，字段长度是 1 字节。指明 ARP 协议报文中物理地址(MAC 地址)的长度，对于大部分网络来说，这个值是 6（6 个字节，即 48 比特）。
4. Protocol Address Length：网络地址长度，字段长度是 1 字节。表示 ARP 协议报文中网络地址（IP 地址）有多少比特，对于大部分网络来说，这个值是 4（4 个字节，即 32 比特。
5. Opcode：操作类型字段，占用 2 个字节，值为 1 代表 ARP 请求报文，值为 2 代表 ARP 应答报文，3 代表 RARP 请求报文，4 代表 RARP 应答报文。
6. Sender Hardware Address：占 6 字节，标识发送方的物理地址（MAC 地址）。
7. Send Protocol Address：占 4 字节，标识发送方的 IP 地址。
8. Target Hardware Address：占 6 字节，表示接收方设备的硬件地址，在请求报文中该字段值全为 0，即 00-00-00-00-00-00，表示任意地址，因为现在不知道这个 MAC 地址。
9. Target Protocol Address：占 4 字节，标识接收方的 IP 地址 。

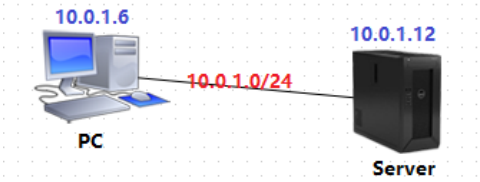
3. ARP 命令

使用 ARP 命令可以显示或修改 ARP 协议使用的高速缓存中 IP 地址和物理地址的映射关系。按照默认设置，ARP 高速缓存中的项目是动态的，每当发送至一个指定地点的数据包且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。Windows 下 ARP 命令的主要参数及含义如下：

1. arp -a [inet_addr] [-N if_addr]: 显示 ARP 缓存信息，即所有已存在的 IP 和 MAC 的对应关系。若指定 IP 地址，则只显示该 IP 地址的 ARP 缓存信息。
2. arp -d inet_addr [if_addr]: 删除所有 ARP 缓存内容。若在命令中指定 IP 地址，则只删除该 IP 地址的 ARP 缓存信息。
3. arp -s inet_addr eth_addr [if_addr]: 向 ARP 高速缓存中人工输入添加静态项目，即增加 IP 地址和物理地址的映射关系。在显示 ARP 缓存信息时，该信息类型为 STATIC。

三 实验环境

在右上方的实验拓扑图菜单中选择 **ARP**，点击连线设置子网网段：



然后点击**提交实验**，等待资源分配成功后，点击图标按全屏访问即可进入设备进行实验(注：Server 账户密码均为 centos)。

四 实验内容

1. ARP 缓存表

进入 PC，打开 cmd，使用 **arp -a** 查看本机的 ARP 缓存：

```
C:\Documents and Settings\admin>arp -a

Interface: 10.0.1.6 --- 0x10003
  Internet Address      Physical Address      Type
  10.0.1.2              fa-16-3e-4f-9a-27     dynamic
```

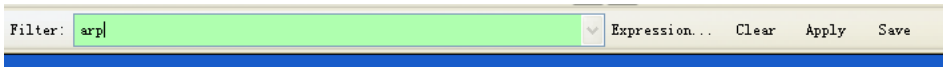
ARP 缓存表中的每一项条目记录了一条 IP 地址到 MAC 地址的映射以及该条映射的类型(dynamic、static)。不同类型的条目的主要区别在于其生命周期不同，静态条目会一直保留在 ARP 缓存中，意思是永久生效。而动态条目随时间推移自动添加和删除:

1. 每个动态 ARP 缓存条目默认的生命周期(TTL)是两分钟。当超过两分钟，该条目会被删掉。所以，生命周期也被称为超时值。
2. 延长规则：当 ARP 条目已存在，使用该条目后，将会重设超时值为两分钟。

可以看到当前 ARP 缓存中并没有关于 Server 的条目。

2. 捕获 ARP 包

打开 PC 中的 Wireshark，在过滤字段中输入 **arp**，再点击右边的 **Apply** 按钮：



接下来选择本地连接网卡，然后点击 Start 按钮开始抓取 ARP 包。在 cmd 中输入命令 **ping 10.0.1.12**，可以看到 wireshark 中捕获到了 ARP 相关的数据包：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	fa:16:3e:a9:19:31	Broadcast	ARP	42	who has 10.0.1.12? Tell 10.0.1.6
2	0.00061800	fa:16:3e:02:42:9a	fa:16:3e:a9:19:31	ARP	42	10.0.1.12 is at fa:16:3e:02:42:9a
11	5.01480500	fa:16:3e:02:42:9a	fa:16:3e:a9:19:31	ARP	42	who has 10.0.1.6? Tell 10.0.1.12
12	5.01488600	fa:16:3e:a9:19:31	fa:16:3e:02:42:9a	ARP	42	10.0.1.6 is at fa:16:3e:a9:19:31

再次查看 PC 中的 ARP 缓存，多出了一条关于 Server 的 IP 地址到 MAC 地址的动态映射条目：

```
C:\Documents and Settings\admin>arp -a

Interface: 10.0.1.6 --- 0x10003
  Internet Address      Physical Address      Type
  10.0.1.12             fa-16-3e-02-42-9a     dynamic
```

3. ARP 分析

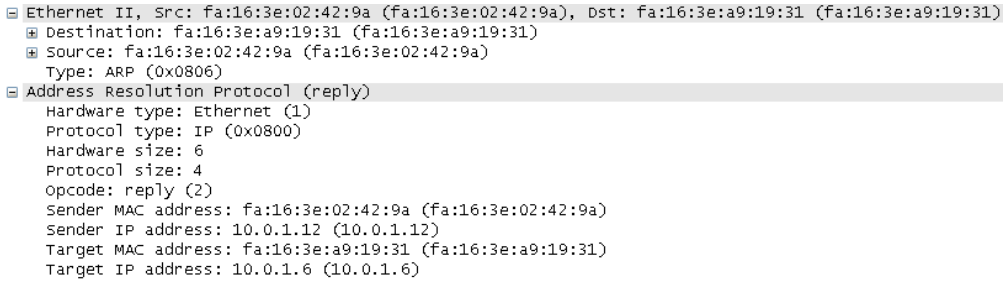
如下图所示，为获取 Server 的 MAC 地址，PC 先进行广播(Broadcast)：

```
⊟ Ethernet II, Src: fa:16:3e:a9:19:31 (fa:16:3e:a9:19:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: fa:16:3e:a9:19:31 (fa:16:3e:a9:19:31)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: fa:16:3e:a9:19:31 (fa:16:3e:a9:19:31)
    Sender IP address: 10.0.1.6 (10.0.1.6)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.1.12 (10.0.1.12)
```

ARP 请求分组(No=1)

请求分组中，PC 将本机的 MAC 地址和 IP 地址信息放入 **Sender MAC address** 和 **Sender IP** 字段。由于此时所请求的 IP 地址对应的 MAC 地址未知，故而 **Target MAC** 字段用全 0 进行填充。该请求分组会被本局域网上的所有运行了 ARP 进程的主机收到，接收到该请求分组的主机会对照本机 IP 地址和 ARP 请求分组中要查询的 IP 地址是否一致，如果一致，便

向源主机发送 ARP 响应分组，因此，Server 接收到请求分组后，根据请求分组中的 IP 地址和 MAC 地址信息向 PC 发送应答分组：



ARP 应答分组(No=2)

同样，应答分组中 Server 也将自己的 MAC 地址和 IP 地址信息填入 ARP 报文中，PC 接收到该应答分组后，便得到了所请求的 Server 的 IP 地址的 MAC 地址信息，随后将该信息存入 ARP 告诉缓存中。接着就可以和 Server 通过 ICMP 进行正常通讯。那么我们是如何区分 ARP 请求和应答分组的呢？分组中的地址字段和其他相同的字段无法作为区分依据，这时 **Opcode** 字段就发挥了作用，根据 Opcode 的值可以确定是请求(**opcode=1**)还是应答(**opcode=2**)，是 ARP 还是 RARP。请同学们结合预备知识分析每个字段的含义。

4. 扩展

依次完成以下实验：

1. 验证 PC 中 ARP 缓存表中的动态条目生命周期为 2 分钟。
2. 使用 ARP 相关命令清空 PC 中的缓存表，然后手动添加一条记录了 Server 的 IP 地址和物理地址信息的静态条目并验证条目的可用性。
3. PC 中使用 ping 命令向同一局域网(同一网段)但不存在的 IP 地址发送数据包，并用 wireshark 分析 ARP 的处理方式。
4. PC 中使用 ping 命令向不同局域网的 IP 地址发送数据包，并用 wireshark 分析 ARP 的处理方式。