实验 23：ARP 消息分析实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/05/16

【实验目的】

1. 理解 ARP 协议的基本原理：学生将通过实验了解 ARP 协议的作用，即如何在以太网环境中将已知的 IP 地址转换为 MAC 地址。这涉及到 ARP 请求和响应消息的生成与处理。
2. 学习 ARP 消息的结构和字段内容:实验将指导学生详细了解 ARP 消息的格式，包括硬件类型、协议类型、硬件地址长度、协议地址长度、操作码、源硬件地址、源协议地址、目标硬件地址以及目标协议地址等字段。
3. 掌握 ARP 映射的静态与动态方式：学生将学习 ARP 协议中静态映射和动态映射的区别和应用场景，理解两者的优缺点以及适用环境。
4. 操作实践与网络工具应用：通过使用网络模拟工具如 Packet Tracer 和网络分析工具如 Wireshark，学生将实际操作 ARP 协议的配置和分析，包括抓取和解析 ARP 数据包。
5. 诊断和解决网络地址问题：通过分析 ARP 数据包，学生可以学习如何诊断网络中的地址解析问题，如 IP 地址和 MAC 地址不匹配、ARP 缓存中的脏数据等。
6. 提高网络安全意识：学生将探索 ARP 协议可能的安全漏洞，如 ARP 欺骗，并学习基本的防护措施。

【实验原理】

一、ARP 协议的出现原因

ARP（地址解析协议）是网络通信中的关键协议。在以太网中，通信依赖于设备的 MAC 地址，而不是 IP 地址。ARP 协议的主要作用是将已知的 IP 地址转换成目标设备的 MAC 地址，以确保数据能够正确传输。主机在进行通信时，需要先确定对方的 MAC 地址，这就是地址解析的过程，由 ARP 来完成。

二、ARP 映射方式

静态映射：管理员手动创建 ARP 表，将 IP 地址和 MAC 地址关联并保存在网络中每台机器上。这种方式有局限性，比如网络适配器的更换或移动电脑的迁移

可能导致物理地址的变化。因此，静态 ARP 表需要定期更新和维护，增加了操作的复杂性。

动态映射：每台主机只需知道对方的 IP 地址，即可使用 ARP 协议查找相应的 MAC 地址。ARP 协议是将 IP 地址映射为 MAC 地址，反向 ARP（RARP）则用于将 MAC 地址映射为 IP 地址。

三、ARP 工作原理及流程

请求：当一台主机想要发送数据给另一台主机时，它首先广播一个 ARP 请求，包含自身的 MAC 和 IP 地址以及目标设备的 IP 地址。由于此时不确定目标 MAC 地址，查询分组会在网络层中广播。

响应：局域网内的所有主机接收并处理这个 ARP 请求。如果某台主机的 IP 地址与请求中目标 IP 地址匹配，它会返回一个 ARP 响应，包含自身的 MAC 地址，以单播方式发送给请求主机。

四、ARP 协议报文字段及抓包分析

1. 报文格式
   - 硬件类型：标识运行 ARP 的网络类型，例如以太网为 1。
   - 协议类型：标识使用的协议，例如 IPv4 为 0800。
   - 硬件长度：表示物理地址的长度（以太网为 6 字节）。
   - 协议长度：表示逻辑地址的长度（IPv4 为 4 字节）。
   - 操作码：标识报文类型（1 为请求，2 为响应）。
   - 源硬件地址：发送方的 MAC 地址（以太网为 6 字节）。
   - 源逻辑地址：发送方的 IP 地址（IPv4 为 4 字节）。
   - 目标硬件地址：目标设备的 MAC 地址（请求时全 0，响应时 6 字节）。
   - 目标逻辑地址：目标设备的 IP 地址（IPv4 为 4 字节）。
2. 报文长度：ARP 报文总长度为 64 字节，包括以太网帧头和 ARP 数据。为了满足以太网最小帧长要求，报文中还添加填充字段。
3. CRC 字段：用于验证以太网帧的正确性。在填充完成后，通过算法计算的值会放入 CRC 字段，接收方可以验证数据包是否被修改。

五、报文封装

ARP 报文直接封装在数据链路帧中，以太网帧的类型字段标识此帧中携带的

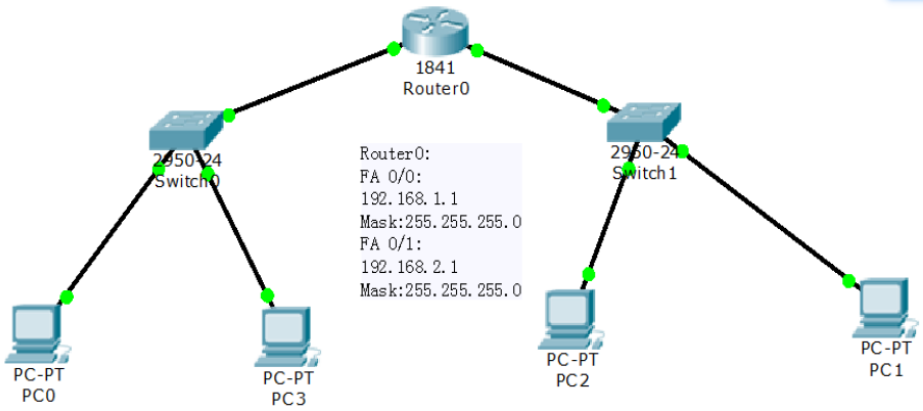
是 ARP 报文。

【实验设备】

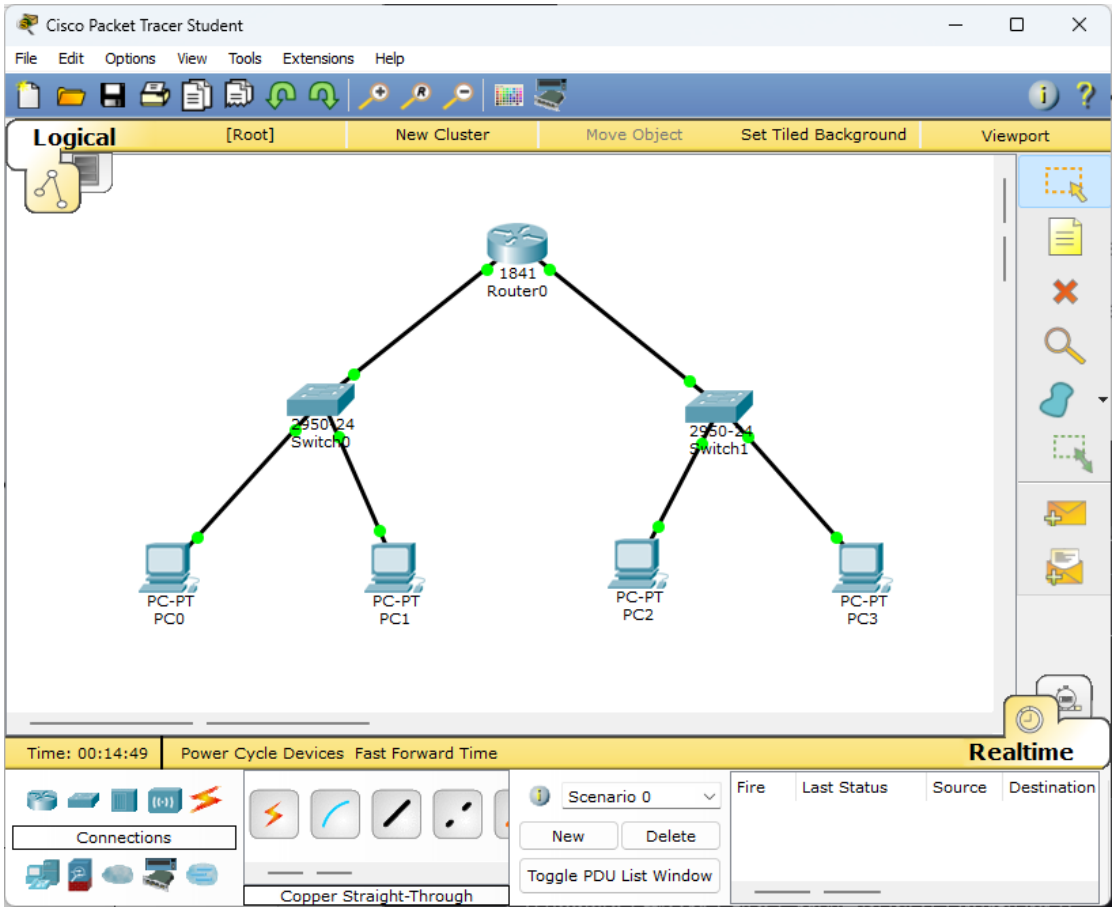
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

【实验步骤】

1. 规划网络地址及拓扑图。



2. 启动 Cisco Packet Tracer，按照上图连接网络，并参照先前实验进行配置。



3. 在 PC 机的命令行中输入如下命令，观察清除 ARP 前后当前主机的 ARP（地址解析协议）表内容。

```
arp -a
arp -d
arp -a
```

4. 在 Router 的 CLI 中输入如下命令，观察清除 ARP 前后当前路由的 ARP（地址解析协议）表内容。

```
show arp
clear arp-cache
show arp
```

5. 从 Realtime 模式切换至 Simulation 模式。

   5.1 在 PC1（192.168.2.13）的命令行中执行命令 ping 192.162.1.11（ping PC0）。

   5.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

   5.3 在 Even List 中的 Info 栏可以查看相关信息。

6. 使用 WireShark 抓取 ARP 数据包，查看 ARP 报文字段内容，并解读。
7. 分析在 Packet Tracer 中 ARP 报文情况。
8. 查看本机的 ARP 内容。

【实验现象】

1. 在 PC 机的命令行中输入如下命令，显示当前主机的 ARP（地址解析协议）表内容。

```
arp -a
```

```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.2.1           00e0.8fac.8302        dynamic
```

2. 在 PC 机的命令行中输入如下命令，清除当前主机的 ARP（地址解析协议）表内容。

```
arp -d
```

3. 在 PC 机的命令行中再次输入如下命令，显示当前主机的 ARP（地址解析协议）表内容。

```
arp -a
```

```
PC>arp -a
No ARP Entries Found
```

4. 在 Router 的 CLI 中输入如下命令，查看当前路由的 ARP（地址解析协议）表内容。

```
show arp
```

```
Router>show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   0007.EC20.5201  ARPA   GigabitEthernet0/0
Internet  192.168.1.13           8   0060.5CD8.8C20  ARPA   GigabitEthernet0/0
Internet  192.168.2.1            -   0007.EC20.5202  ARPA   GigabitEthernet0/1
Internet  192.168.2.11           8   00D0.BC2C.850B  ARPA   GigabitEthernet0/1
Internet  192.168.2.12           7   0010.1123.C50E  ARPA   GigabitEthernet0/1
```

5. 在 Router 的 CLI 中输入如下命令，清除当前路由的 ARP（地址解析协议）表内容。

```
clear arp-cache
```

6. 在 Router 的 CLI 中再次输入如下命令，查看当前路由的 ARP（地址解析协议）表内容。

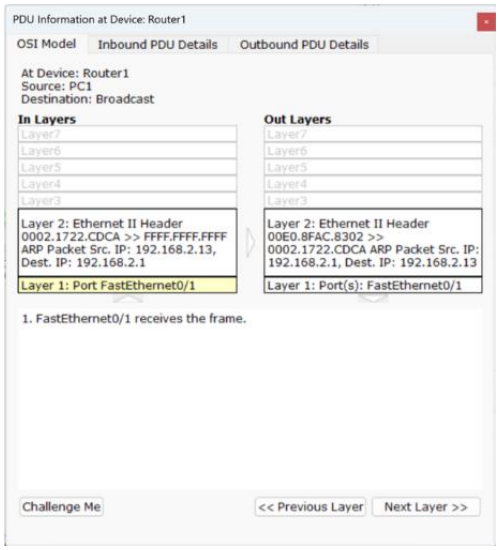
```
show arp
```

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.13           -   Incomplete      ARPA   GigabitEthernet0/0
Internet  192.168.2.11           -   Incomplete      ARPA   GigabitEthernet0/1
Internet  192.168.2.12           -   Incomplete      ARPA   GigabitEthernet0/1
Internet  192.168.1.1            -   0007.EC20.5201  ARPA   GigabitEthernet0/0
Internet  192.168.2.1            -   0007.EC20.5202  ARPA   GigabitEthernet0/1
```

【分析讨论】

一、使用 WireShark 抓取 ARP 数据包，查看 ARP 报文字段内容，并解读

1. PDU Information at Device: Router1（OSI Model）



这张图展示了一个典型的网络数据包在路由器处理中的入站和出站信息，特

别是针对 ARP（地址解析协议)请求的处理。这个图中详细地描述了 OSI 模型中的不同层级如何处理 ARP 请求和响应。

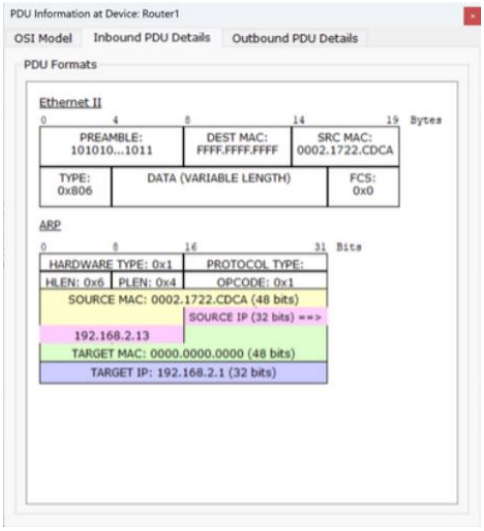
左侧（Inbound PDU Details)：

- At Device: Router1：显示该信息来自 Router1 设备。
- Source：PC1：数据包源自 PC1。
- Destination：Broadcast：这是一个广播包，目标是所有设备。
- Layers：
  - Layer 1：物理层，指出数据包通过 Router1 的 FastEthernet0/1 端口接收。
  - Layer 2：数据链路层，展示了 Ethernet II 帧头信息。源 MAC 地址为 0002.1722.CDCA，目标 MAC 地址为广播地址 FFFF.FFFF.FFFF。ARP 请求包的源 IP 为 192.168.2.13，目标 IP 为 192.168.2.1。

右侧（Outbound PDU Details)：

- 同样在 Router1 设备上显示出站的 PDU（协议数据单元）细节。
- Layers：
  - Layer 1：物理层，数据包通过相同的 FastEthernet0/1 端口发送出去。
  - Layer 2：数据链路层，显示了 Ethernet II 帧头信息。此时源 MAC 地址为 000E.8FAC.8302，目标 MAC 地址为 0002.1722.CDCA。ARP 响应的源 IP 为 192.168.2.1，目标 IP 为 192.168.2.13。

2. PDU Information at Device: Router1（Inbound PDU Details）



这张图详细展示了在Router1设备上接收的ARP请求的协议数据单元(PDU)的格式。具体内容分为Ethernet II帧格式和ARP协议部分，下面是各部分的详细解释：

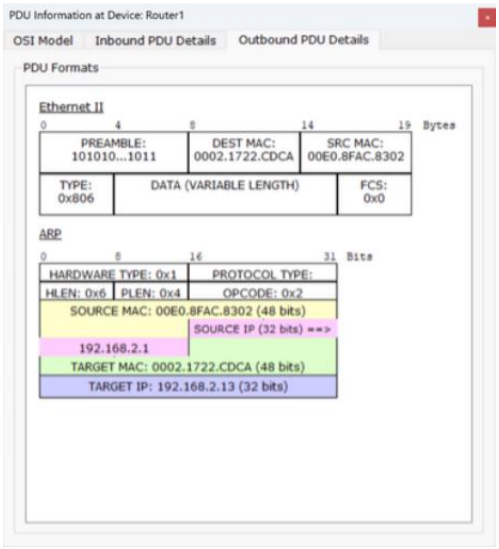
Ethernet II：

- Preamble（前导码）：起始部分为101010...1011，这部分用于同步网络设备之间的时钟频率，以确保数据的正确解读。
- Destination MAC（目标MAC地址）：为FFFF.FFFF.FFFF，这是一个广播地址，表示该ARP请求被发送到所有设备。
- Source MAC（源MAC地址）：为0002.1722.CDCA，这是发送该请求的设备的物理地址。
- Type（类型）：0x806，表示这个帧携带的数据是ARP协议的数据。
- Data（数据）：数据部分是可变长度的，包括ARP请求的具体内容。
- FCS（帧检验序列）：为0x0，用于错误检测的帧尾，虽然在此图示中显示为0，实际操作中由网络设备计算并添加。

ARP：

- Hardware Type（硬件类型）：0x1，表示这是以太网（Ethernet）。
- Protocol Type（协议类型）：0x0800，表示上层协议是IP。
- HLEN（硬件地址长度）：0x06，表示硬件地址（MAC地址）的长度为6字节。
- PLEN（协议地址长度）：0x04，表示协议地址（IP地址）的长度为4字节。
- Opcode（操作码）：0x01，表示这是一个ARP请求（请求MAC地址）。
- Source MAC Address：0002.1722.CDCA，请求方的物理地址。
- Source IP Address：192.168.2.13，请求方的IP地址。
- Target MAC Address：0000.0000.0000，目标方的MAC地址在请求时未知，因此全为0。
- Target IP Address：192.168.2.1，目标方的IP地址，即发送方希望获取MAC地址的IP地址。

3. PDU Information at Device: Router1（Outbound PDU Details）



这张图展示了从 Router1 发出的一个 ARP 响应的协议数据单元（PDU）的详细信息。这是对之前 ARP 请求的回应，具体内容如下：

Ethernet II：

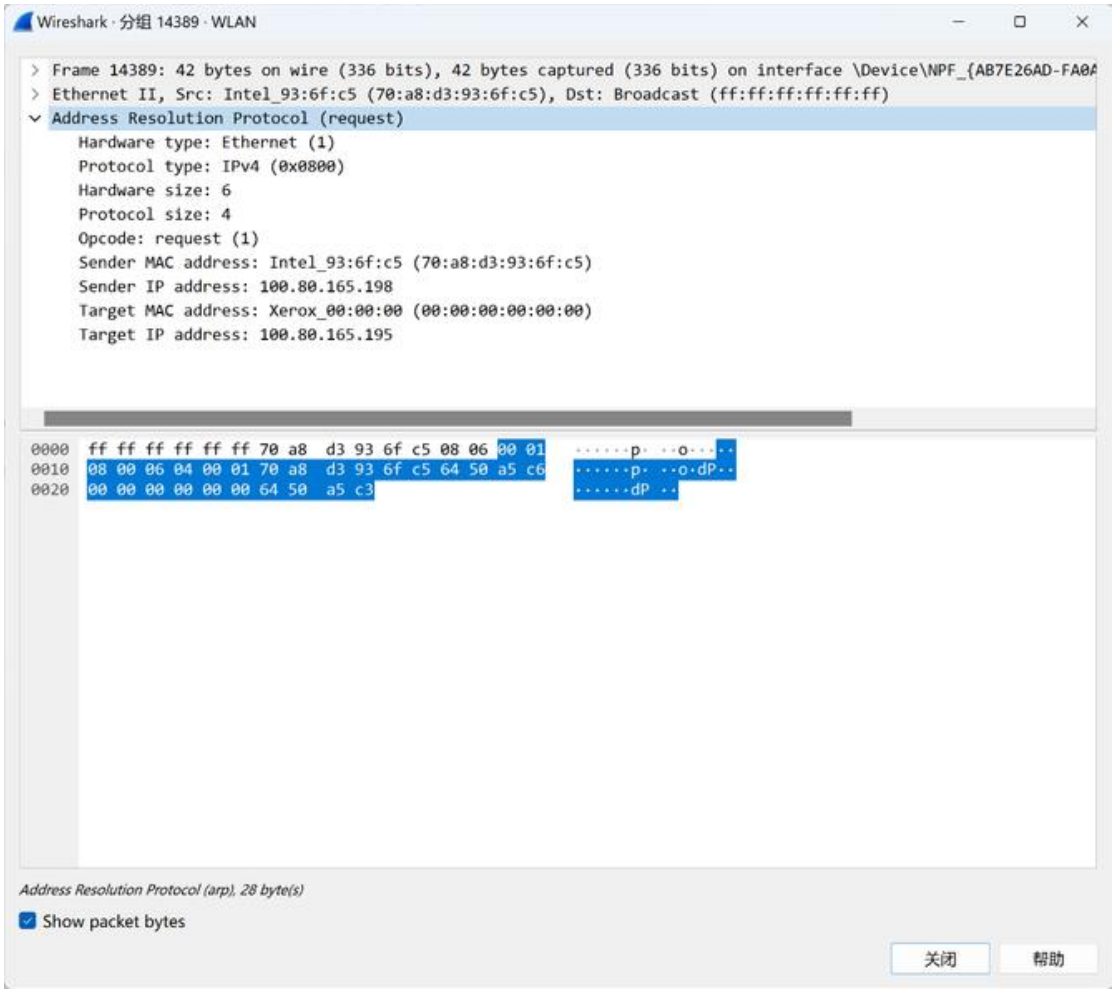
- Preamble（前导码）：为 101010...1011，用于时钟同步，以确保接收方能正确解析接下来的数据。
- Destination MAC（目标 MAC 地址）：为 0002.1722.CDCA，即发出 ARP 请求的设备的物理地址。
- Source MAC（源 MAC 地址）：为 00E0.8FAC.8302，即响应 ARP 请求的设备的物理地址。
- Type（类型）：0x806，指明这是一个 ARP 协议的数据包。
- Data（数据）：包含了 ARP 响应的详细内容。
- FCS（帧检验序列）：0x0，用于错误检测的帧尾，在此图中为示意，实际中会由设备计算并添加。

ARP：

- Hardware Type（硬件类型）：0x1，表示此 ARP 响应是针对以太网环境的。
- Protocol Type（协议类型）：0x0800，表示协议是 IP。
- HLEN（硬件地址长度）：0x06，表示硬件地址（MAC 地址）长度为 6 字节。
- PLEN（协议地址长度）：0x04，表示协议地址（IP 地址）长度为 4 字节。
- Opcode（操作码）：0x02，表示这是一个 ARP 响应。

- Source MAC Address：00E0.8FAC.8302，响应方的物理地址。
- Source IP Address：192.168.2.1，响应方的 IP 地址。
- Target MAC Address：0002.1722.CDCA，目标方（即请求方）的物理地址。
- Target IP Address：192.168.2.13，目标方的 IP 地址。

二、分析在 Packet Tracer 中 ARP 报文情况



下面对 Packet Tracer 中 ARP 报文情况进行分析：

Ethernet II：

- 源 MAC 地址：Intel_93:6f:c5（70:a8:d3:93:6f:c5）发送 ARP 请求的设备的物理地址。
- 目的 MAC 地址：Broadcast（ff:ff:ff:ff:ff:ff）表明这是一个广播消息，所有在网络上的设备都会接收这个包。
- 类型：0x0806 表示这个帧是 ARP 数据包。

ARP 报文：

- 硬件类型：1（Ethernet），这表明 ARP 请求是在以太网环境中使用的。
- 协议类型：0x0800（IPv4），这表明 ARP 请求是为了解析 IPv4 地址。
- 硬件地址长度：6，指出 MAC 地址使用 6 个字节。
- 协议地址长度：4，指出 IPv4 地址使用 4 个字节。
- 操作码：1（request），这表示此 ARP 包是一个请求包。
- 发送者 MAC 地址：Intel_93:6f:c5（70:a8:d3:93:6f:c5）同 Ethernet 头部的源地址。
- 发送者 IP 地址：100.80.165.198，发起 ARP 请求的设备的 IP 地址。
- 目标 MAC 地址：00:00:00:00:00:00，在请求时目标 MAC 地址未知，通常设置为全零。
- 目标 IP 地址：100.80.165.195，发起 ARP 请求的设备希望得到此 IP 地址的 MAC 地址。

三、查看本机的 ARP 内容

```
C:\Users\lenovo>arp -a

接口: 192.168.178.1 --- 0x2
  Internet 地址         物理地址              类型
  192.168.178.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 100.81.138.91 --- 0x6
  Internet 地址         物理地址              类型
  100.81.255.254        9c-54-c2-0d-50-02     动态
  100.81.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.216.1 --- 0x1b
  Internet 地址         物理地址              类型
  192.168.216.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

在 Windows 命令提示符中输入 arp -a，我们可以看到三个网络接口的 ARP

表信息。每个接口列出了与之相关联的 IP 地址、相应的物理地址（MAC 地址）和条目类型（静态或动态）。以下是各部分的具体解释：

1. 接口：192.168.178.1 --- 0x2
   - IP 地址 192.168.178.255：这是一个子网广播地址，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态，表示这个地址是用于广播消息到本地网络上的所有设备。
   - IP 地址 224.0.0.22，224.0.0.251，224.0.0.252：这些都是多播地址，对应的 MAC 地址以 01-00-5e 开头，根据多播 IP 到 MAC 地址映射的标准来设定，也都是静态条目。
   - IP 地址 239.255.255.250:同样是一个多播地址,用于特定的多播服务，如 SSDP（简单服务发现协议），MAC 地址同样为静态。
2. 接口：100.81.138.91 --- 0x6
   - IP 地址 100.81.255.254:这个地址可能是该接口的默认网关或者某个特定服务的地址，MAC 地址为 9c-54-c2-0d-50-02，标记为动态，表示这个地址是从网络上动态学习的。
   - IP 地址 100.81.255.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。
   - 其余 IP 地址：包括多播地址和广播地址，与第一个接口的描述相同。
3. 接口：192.168.216.1 --- 0x1b
   - IP 地址 192.168.216.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。
   - 其余 IP 地址：包括多播地址和广播地址，与前面的接口描述相同。

四、实验现象分析与讨论

1. ARP 表的初步观察

在使用 arp -a 命令查看 ARP 表时，可以看到本机已知的网络设备的 IP 地址和 MAC 地址列表。这显示了当前设备已经学习到的网络内部的 IP 到 MAC 地址映射。

2. 清除 ARP 缓存后的变化

执行 arp -d 清除 ARP 缓存后，再次使用 arp -a 查看 ARP 表时，表中内容减

少或显示为空。清除 ARP 缓存后，本机删除了所有动态学习的 IP 到 MAC 地址映射。这表明 ARP 缓存是动态的，设备通过网络通信实时更新这些信息。

3. ARP 缓存自动恢复

一段时间后，再次使用 arp -a 命令，发现 ARP 表已经重新填充了一些条目。这说明操作系统和网络设备在网络活动中自动重新学习了 IP 到 MAC 的映射这可能通过 ARP 请求和响应，或通常的网络交互过程自动完成。

4. 模拟 ARP 请求和响应

在 Cisco Packet Tracer 或 Wireshark 中模拟并抓取 ARP 数据包，观察到发送 ARP 请求后，接收到了 ARP 响应。这一现象验证了 ARP 协议的工作机制。请求被发送到广播地址，网络上所有设备均接收此请求，但只有 IP 地址匹配的设备才回应其 MAC 地址，这是典型的 ARP 查询流程。