**实验三：验证地址解析协议ARP的工作过程**

1. **实验名称**

验证地址解析协议ARP的工作过程

1. **实验目的**

1、了解ARP协议的基本知识和工作原理；

2、学习使用ARP命令；

3、研究ARP欺诈的机制。

1. **实验完成人及完成时间**

史文翰

No.2014211218

Cla.2014211304

2016.10.27

1. **实验环境**

与Internet连接的笔记本电脑，Win10操作系统。

在同一局域网内的两台主机（具体的IP和MAC在实验步骤中给出）

在做（1）时，配置如下：

**A主机（默认配置）：**

**MAC：80-FA-5B-01-C6-8F**

**IPv4：10.206.32.201**

**B主机（默认配置）**

**MAC：30-65-EC-19-2D-65**

**IPv4：10.206.32.210**

在做之后的实验时，为了配合掩码的设计，更改它们的IPv4地址如下：

**A主机（更改之后的配置）：**

**IPv4：10.2.2.2**

**子网掩码：255.255.255.0**

**注：10.2.2.X and 255.255.255.0 = 10.2.2.0**

**10.2.3.X and 255.255.255.0 = 10.2.3.0（不同，判断不在同一个网段）**

**B主机（更改之后的配置）：**

**IPv4：10.2.3.3**

**子网掩码：255.255.254.0**

**注：10.2.2.X and 255.255.254.0 = 10.2.2.0**

**10.2.3.X and 255.255.254.0 = 10.2.2.0（相同，判断在同一个网段）**

这样做是为了在A配置子网掩码255.255.255.0，B配置子网掩码为255.255.254.0之后，在A的角度上判断A与B不在同一个网段，但在B的角度上A与B在同一个网段上，以此来作为（2）实验的背景。

1. **实验步骤与结果分析**

通过设计一个简单的实验来深入直观地理解上述几个知识点所涉及的基本概念与原理。在实验中，利用ping命令来检验主机间能否进行正常的双向通信。在"ping"的过程中，源主机向目标主机发送ICMP的Echo Request报文，目标主机收到后，向源主机发回ICMP的Echo Reply报文，从而可以验证源与目标主机能否进行正确的双向通信。实验的拓扑结构： 如图（1）所示（其中网关和web server的IP地址可以根据情况进行设置）。

1. **设置两台主机的IP地址与子网掩码,两台主机均不设置缺省网关。用arp -d命令清除两台主机上的ARP表，然后在A与B上分别用ping命令与对方通信，用arp -a命令可以在两台PC上分别看到对方的MAC地址。**

首先查看双方主机的MAC地址，本机为



本机IP为



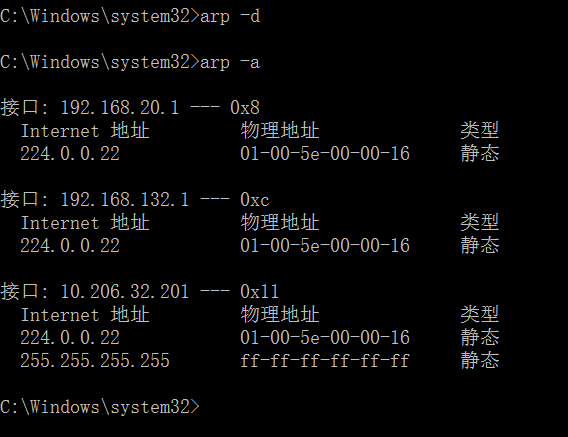
对方的MAC地址为

F:\Tencent Data\191063623\Image\C2C\A[)%]3RX_H6)TUQ]))0~(TB.png

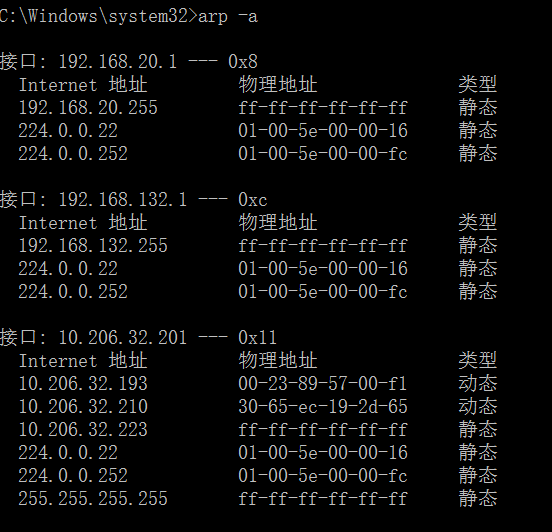
对方IP为



用arp -d 命令删除本机arp表项后

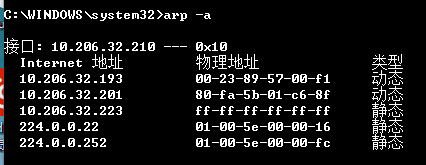


ping对方ip后重新使用arp-a命令查看



黄线指示可以看出已经得到了对方的MAC地址。

从对方角度来看



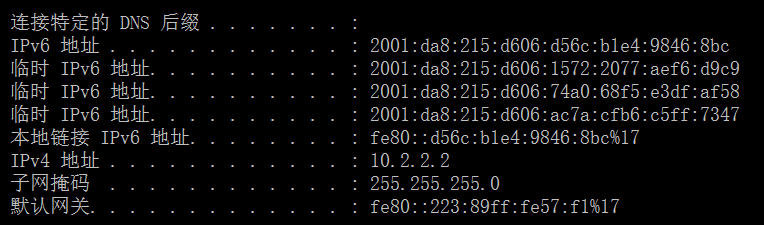
绿线指示了本机的IP和MAC，均正确，说明ARP过程正确执行。

1. **将A的子网掩码改为：255.255.255.0，其他设置保持不变。**

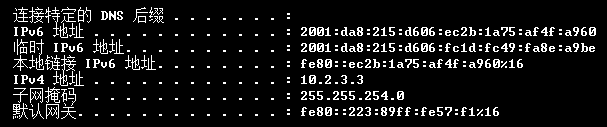
操作1：用arp -d命令清除两台主机上的ARP表，然后在A上"ping"B，观察并分析结果。用arp -a命令在两台PC上均不能看到对方的MAC地址。

首先**我们重新进行配置（以配合实验目的），更改AB两机的IP和掩码后**，内容如下图

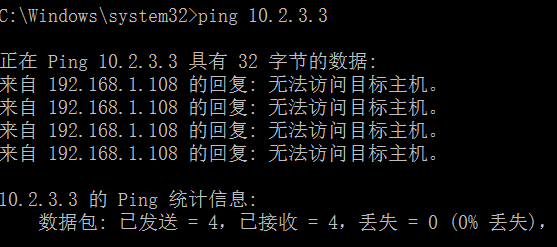
A主机为



B主机为

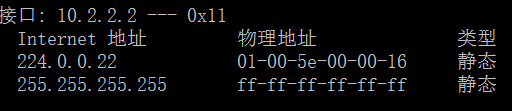


之后用A ping B为



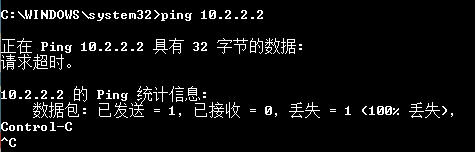
显示“无法访问目标主机”，这是由于子网掩码的设置使得A认为B不在自己的网段上，即**10.2.3.3AND255.255.255.0 = 10.2.3.0，这与10.2.2.0不同**，即判断不在同一个网段上。

查看自身的ARP表



并没有发现B主机的MAC地址

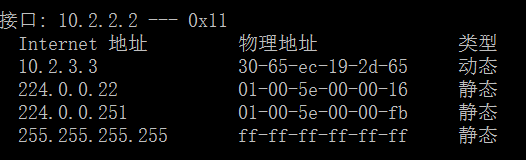
操作2：接着在B上"ping"A，观察并分析结果。



可以看出B的请求包确实已经发送到A上，而非显示的是不可达，这是因为B判断出A在自己的网段上**（10.2.2.2AND255.255.254.0 = 10.2.2.0而10.2.3.3AND255.255.254.0 = 10.2.2.0结果是相同的）**，但是由于A无法向B回送应答包，因此B无法接收到来自A的应答，因此显示的是“请求超时”而非“目的不可达”。

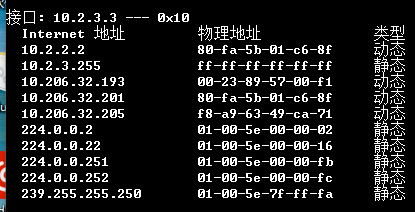
操作3：用arp -a命令可以在两台PC上分别看到对方的MAC地址。

A主机为



可见发现了B主机

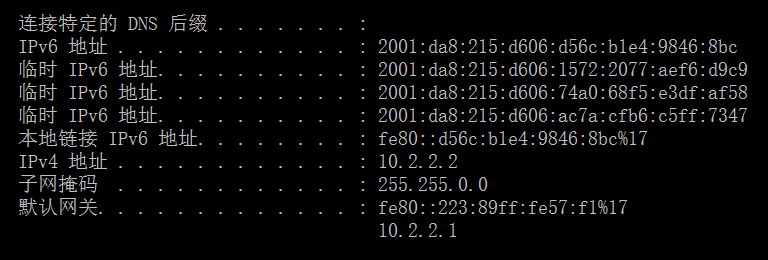
B主机为



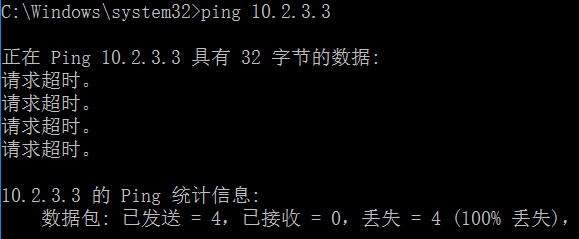
可见发现了A主机

1. **在前面实验的基础上，设置A的缺省网关并将网关的子网掩码为255.255.0.0。在A与B上分别用ping命令与对方通信，观察并分析各自的显示结果。在A与B上分别用tracert命令追踪数据的传输路径，观察显示结果。**

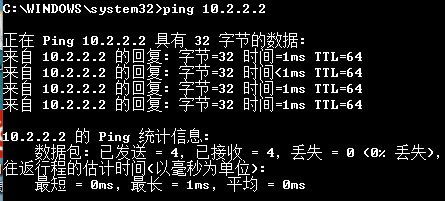
更改A主机的子网掩码



用A ping B有



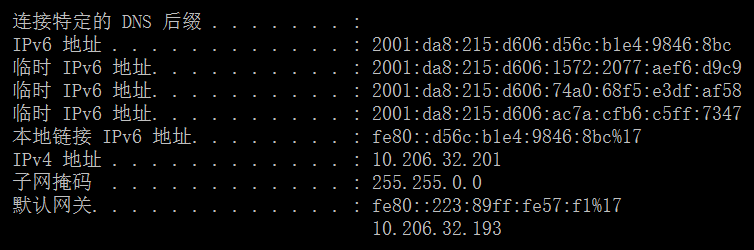
用B ping A有



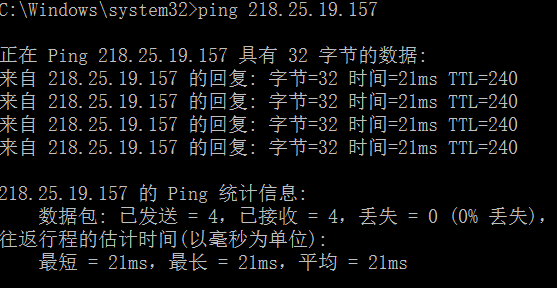
可见A ping B可达但B无法返回一个包给A，但是B ping A可达且这个回声包可以返回。当被识别为在同一个网段时，如果对方设置了正确的默认网关，就可以收到返回的回声包（而像上一题被判断不在同一网段时，直接显示目的不可达）。

1. **用arp -d命令清除A中的ARP表，在A上ping一台外网段的主机，再用arp -a可观察到A的ARP表中只有缺省网关的MAC地址信息。**

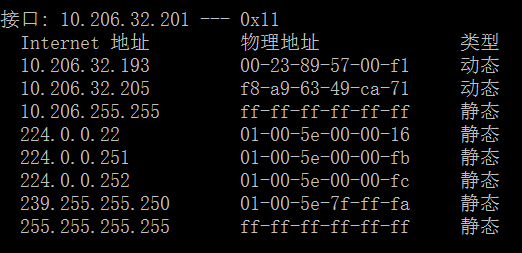
进行如下的设置



利用在实验一中的外网IP



再查看arp表有



可以看出我们网关的MAC地址，而不含外网段目标IP的MAC地址。

**MAC地址欺诈实验设计：当网络中具有不同IP地址的多个主机拥有相同的MAC地址时，网络的通信会发生混乱，这就是MAC欺诈。那么如何进行MAC欺诈呢？请同学利用前面实验学到的网络命令设计一个实验步骤，使主机A、B各自具有不同的IP地址，但MAC地址相同。**

答：当A与C进行通信的时候，如果B作为中间人介入，只需要截获A向C发送的ARP请求包，然后向A回送ARP应答包，其中的MAC地址改写为C的MAC地址，这样B就和C“拥有”相同的MAC地址（在A看来），从而造成了ARP欺骗。A在接下来的通讯中仿佛觉得在和C通信，其实是在和一个伪装成C的B通信。

1. **分析与思考**
2. **以太网地址比IPv4地址多多少位？可以表示出多少个唯一的MAC地址？**

IPV4共32位，MAC共48位。

共可表示2^48个不同的MAC地址。

**2．当使用DHCP为主机分配IP地址时，如果某两台主机具有相同的MAC地址，DHCP server如何给其分配不同的IP地址？**

DHCP会分配相同的IP地址从而造成网络冲突。

**3 . 比较IPv6使用的邻机发现地址解析方法与ARP有什么不同？**

IPV6的获得MAC地址的方式通过ICMPV6的数据包来完成。其实邻居发现协议整合了ARP协议，ICMP路由发现协议和ICMP重定向协议。路由发送报文本身携带MAC地的信息，因此不需要别的机制或者附加报文的交换来解析链路层的MAC地址。