实验四 地址解析协议 (ARP)

地址表

本练习不包括地址表。

学习目标

- 使用 Packet Tracer 的 **arp** 命令
- 使用 Packet Tracer 检查 ARP 交换

简介：

TCP/IP 使用地址解析协议 (ARP) 将第 3 层 IP 地址映射到第 2 层 MAC 地址。当帧进入网络时，必定有目的 MAC 地址。为了动态发现目的设备的 MAC 地址，系统将在 LAN 上广播 ARP 请求。拥有该目的 IP 地址的设备将会发出响应，而对应的 MAC 地址将记录到 ARP 缓存中。LAN 上的每台设备都有自己的 ARP 缓存，或者利用 RAM 中的一小块区域来保存 ARP 结果。 ARP 缓存定时器将会删除在指定时间段内未使用的 ARP 条目。具体时间因设备而异。例如，有些 Windows 操作系统存储 ARP 缓存条目的时间为 2 分钟，但如果该条目在这段时间内被再次使用，其 ARP 定时器将延长至 10 分钟。

ARP 是性能折衷的极佳示例。如果没有缓存，每当帧进入网络时，ARP 都必须不断请求地址转换。这样会延长通信的延时，可能会造成 LAN 拥塞。反之，无限制的保存时间可能导致离开网络的设备出错或更改第 3 层地址。网络工程师必须了解 ARP 的工作原理，但可能不会经常与协议交互。ARP 是一种使网络设备可以通过 TCP/IP 协议进行通信的协议。如果没有 ARP，就没有建立数据报第 2 层目的地址的有效方法。但 ARP 也是潜在的安全风险。例如，ARP 欺骗或 ARP 中毒就是攻击者用来将错误的 MAC 地址关联放入网络的技术。攻击者伪造设备的 MAC 地址，致使帧发送到错误的目的地。手动配置静态 ARP 关联是预防 ARP 欺骗的方法之一。您也可以在 Cisco 设备上配置授权的 MAC 地址列表，只允许认可的设备接入网络。

任务 1：使用 Packet Tracer 的 arp 命令

步骤 1. 访问命令提示符窗口。

单击 PC-1A 的 **Desktop（桌面）**中的 **Command Prompt（命令提示符）**按钮。**arp** 命令只显示 Packet Tracer 中可用的选项。

步骤 2. 使用 ping 命令在 ARP 缓存中动态添加条目。

ping 命令可用于测试网络连通性。通过访问其它设备，ARP 关联会被动态添加到 ARP 缓存中。在 PC-1A 上 ping

地址 255.255.255.255，并发出 arp -a 命令查看获取的 MAC 地址。

任务 2：使用 Packet Tracer 检查 ARP 交换

步骤 1. 配置 Packet Tracer 捕获数据包。

进入模拟模式。确认 Event List Filters（事件列表过滤器）只显示 ARP 和 ICMP 事件。

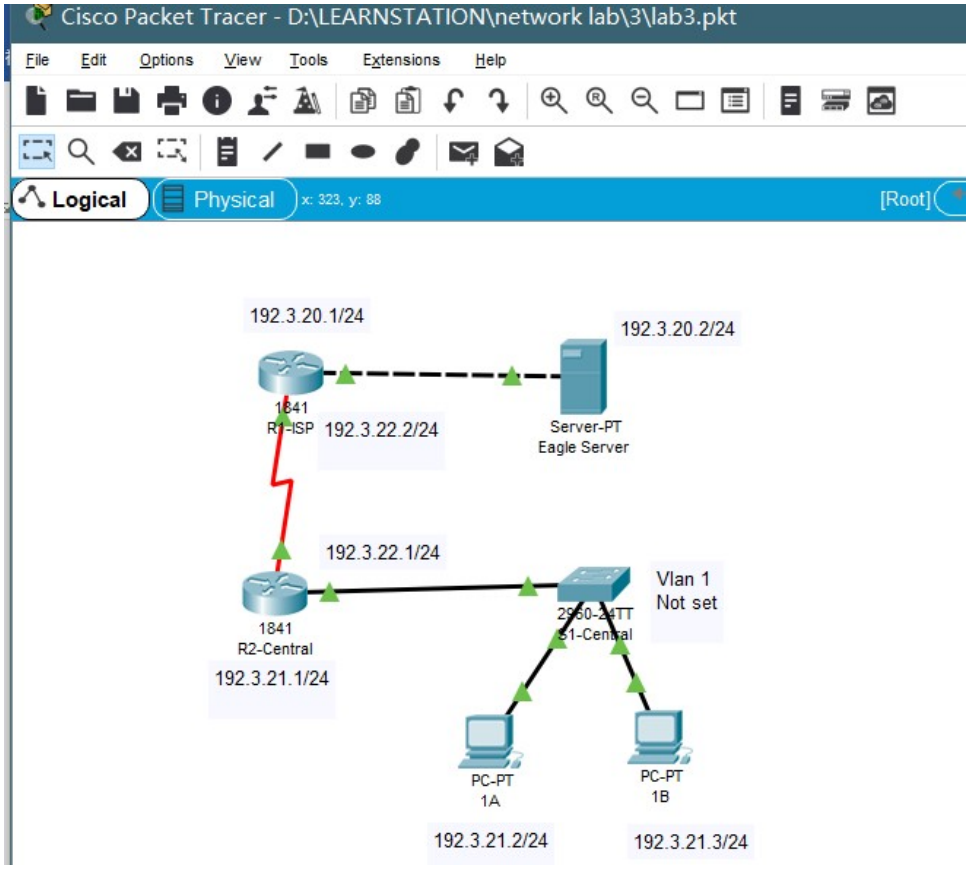
步骤 2. 准备 Pod 主机计算机以执行 ARP 捕获。

在 PC-1A 上使用 Packet Tracer 命令 arp -d。 然后 Ping 地址 255.255.255.255。

步骤 3. 捕获并评估 ARP 通信。

在发出 ping 命令之后，单击 Auto Capture/Play（自动捕获/播放）捕获数据包。当 Buffer Full（缓冲区已满）窗口打开时，单击 View Previous Events（查看以前的事件）按钮。

实例连接图如下：



配置信息：

设备名称	端 口 名称	IP 地址	子网掩码	网关	其他配置
R1-ISP	F0/0	192.3.20.1/24	255.255.255.0	无	无
	S0/0/0	192.3.22.2/24	255.255.255.0	无	Clock Rate=64000 开启动态路由 RIP 协议 版本 V2,no summary 模式 RIP 协议设置网段： 192.3.20.0 192.3.21.0 192.3.22.0
R2-Centeral	F0/0	192.3.21.1/24	255.255.255.0	无	无
	S0/0/0	192.3.22.1/24	255.255.255.0	无	Clock Rate=64000 开启动态路由 RIP 协议 版本 V2,no summary 模式 RIP 协议设置网段： 192.3.20.0 192.3.21.0 192.3.22.0
S1-Central	VLAN 1	未设置	未设置	未设置	无
PC1	NIC	192.3.21.2/24	255.255.255.0	192.3.21.1	无
PC2	NIC	192.3.21.3/24	255.255.255.0	192.3.21.1	无
Eagle Server	NIC	192.3.20.2/24	255.255.255.0	192.3.20.1	

路由器 CLI 进入特权模式（enable）

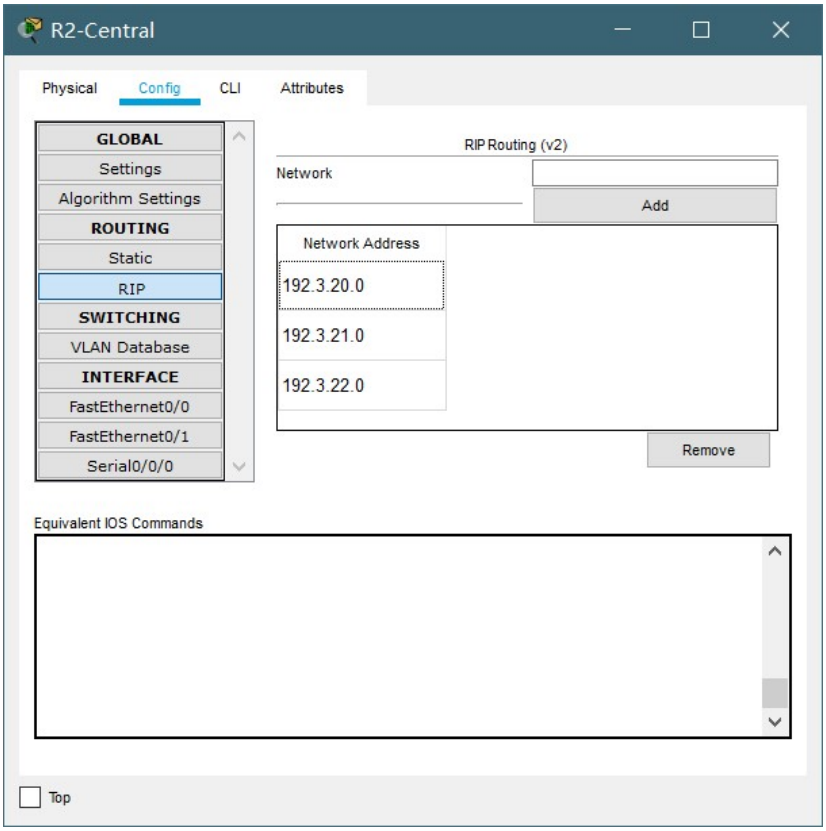
路由器 R1-ISP 设置 RIP 协议（**感谢刘洪驰同学**）

```
Router#config  t
Router(config)# router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network  192.3.20.0
Router(config-router)#network  192.3.21.0
Router(config-router)#network  192.3.22.0
```

路由器 R2-Centeral 设置 RIP 协议

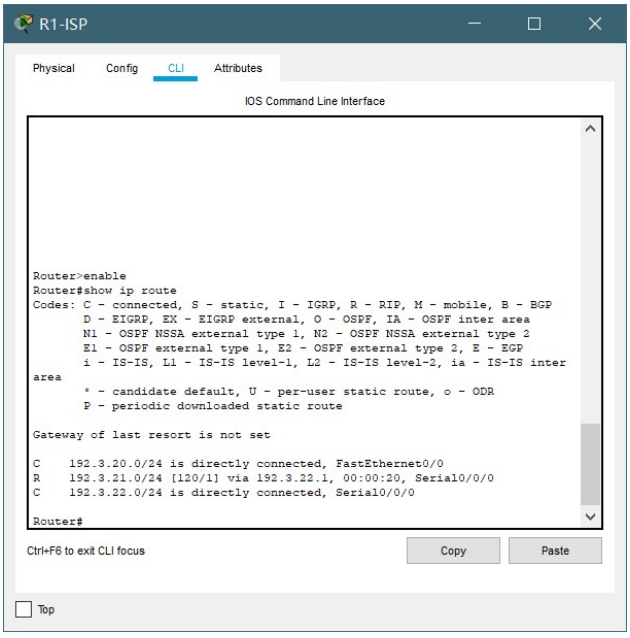
```
Router#config  t
Router(config)# router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network  192.3.20.0
Router(config-router)#network  192.3.21.0
Router(config-router)#network  192.3.22.0
```

RIP 设置截图（部分）



其余设置按照实验 1 照上表设置，不再重复

查看路由工作状态 show ip route



电脑 ping 服务器 192.3.20.2

```
C:\>ping 192.3.20.2

Pinging 192.3.20.2 with 32 bytes of data:

Reply from 192.3.20.2: bytes=32 time=2ms TTL=126
Reply from 192.3.20.2: bytes=32 time=2ms TTL=126
Reply from 192.3.20.2: bytes=32 time=1ms TTL=126
Reply from 192.3.20.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.3.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Top

电脑 ping 255.255.255.255 地址，提示不可达，网上解释说，为了安全，所有新设备都屏蔽了该地址

```
C:\>ping 255.255.255.255
Ping request could not find host 255.255.255.255. Please check the name and try again.
C:\>
```

Top

电脑清除 arp 路由表 arp -d，并且显示路由表为空 arp -a

```
C:\>arp -d
C:\>arp -a
No ARP Entries Found
C:\>
```

Top

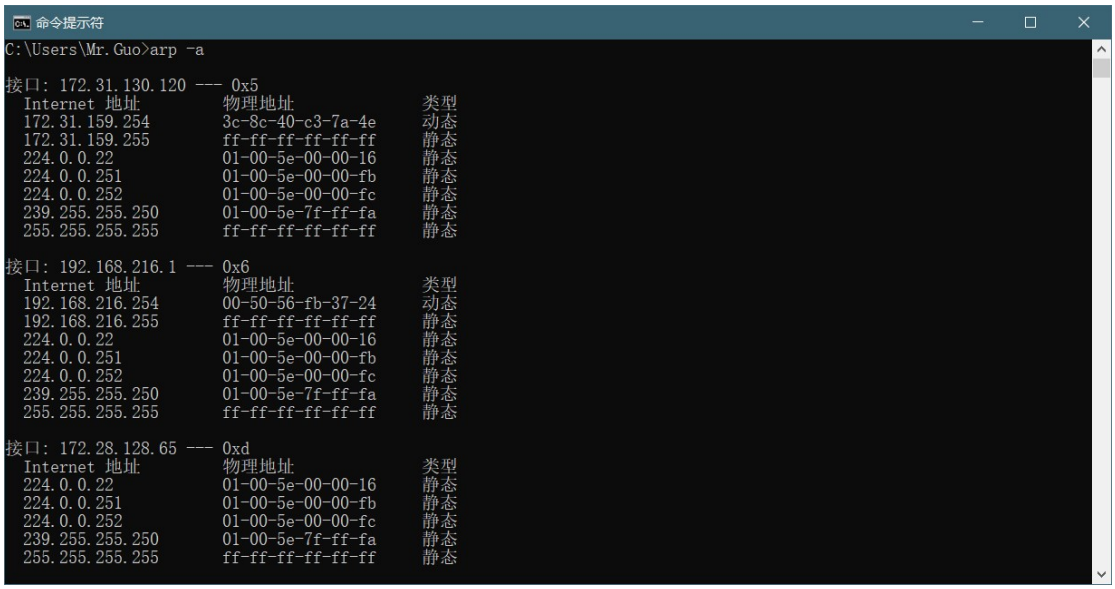
电脑 ping 本网段广播地址 192.3.21.255

```
C:\>arp -d
C:\>arp -a
No ARP Entries Found
C:\>ping 192.3.21.255

Pinging 192.3.21.255 with 32 bytes of data:

Reply from 192.3.21.1: bytes=32 time<1ms TTL=255
Reply from 192.3.21.3: bytes=32 time<1ms TTL=128
Reply from 192.3.21.1: bytes=32 time<1ms TTL=255
Reply from 192.3.21.3: bytes=32 time=1ms TTL=128
Reply from 192.3.21.1: bytes=32 time<1ms TTL=255
Reply from 192.3.21.3: bytes=32 time<1ms TTL=128
Reply from 192.3.21.3: bytes=32 time<1ms TTL=128
Reply from 192.3.21.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.3.21.255:
    Packets: Sent = 4, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

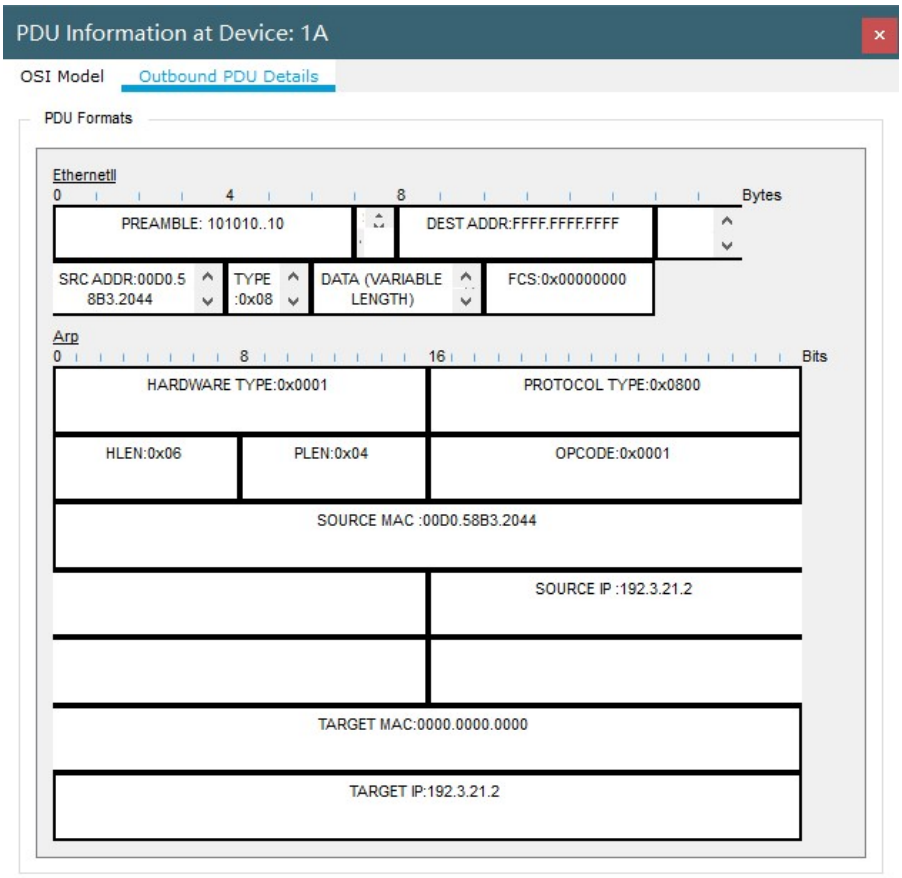
电脑 ping 本网段另一台电脑 192.3.21.3 并查看路由表，只会显示上一跳路由和本网段另一台电脑 MAC 地址，无法获取不同网段的 MAC 地址（由路由负责转发处理）

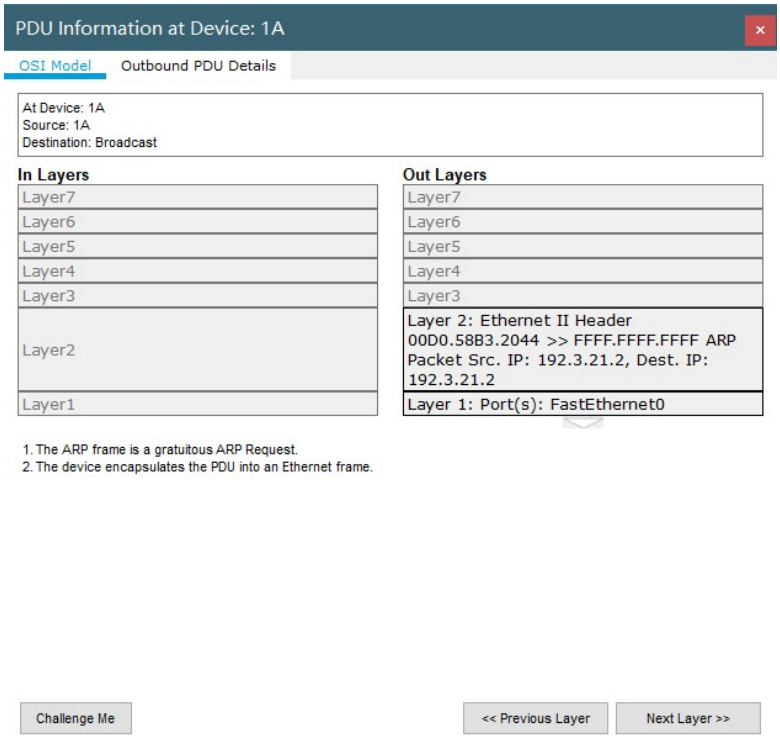
```
C:\>ping 192.3.21.3

Pinging 192.3.21.3 with 32 bytes of data:

Reply from 192.3.21.3: bytes=32 time<1ms TTL=128
Reply from 192.3.21.3: bytes=32 time=3ms TTL=128
Reply from 192.3.21.3: bytes=32 time<1ms TTL=128
Reply from 192.3.21.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.3.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.3.21.1            00d0.582e.1401        dynamic
  192.3.21.3            000b.beae.d8ed        dynamic

C:\>
```

在实际情况下，一些交换机和路由同样为了安全会禁止掉 ping 相同网段的电脑主机，以及 ARP 相关报文，只会得到上一跳的路由地址。



ARP 协议模拟截图





可以看到 MAC 地址都是 FFFF.FFFF.FFFF 代表广播地址。