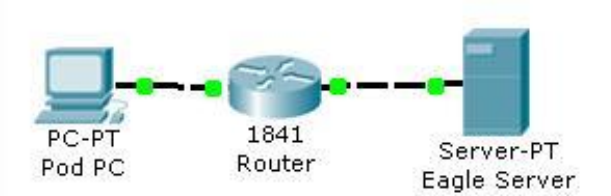
## 实验5、研究ICMP数据包

**拓扑图如下：**

****

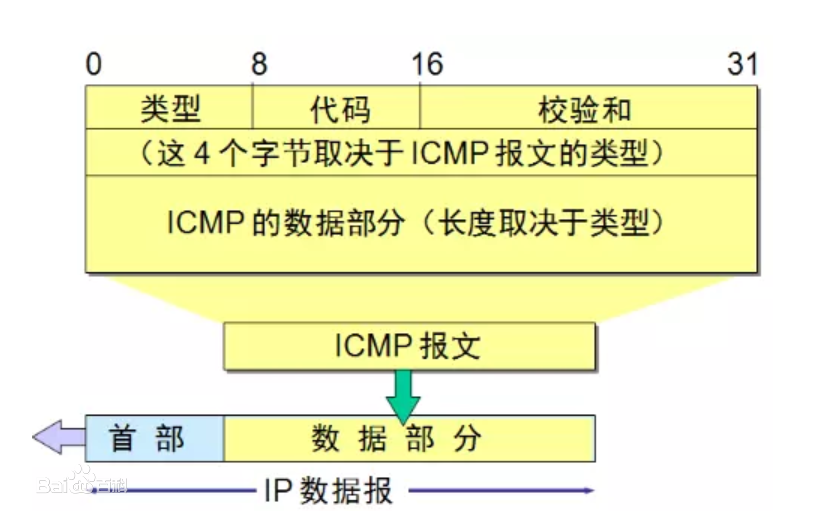
学习目标

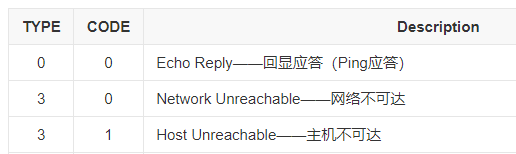
了解ICMP数据包的格式

使Packet Tracer捕获并研究ICMP报文

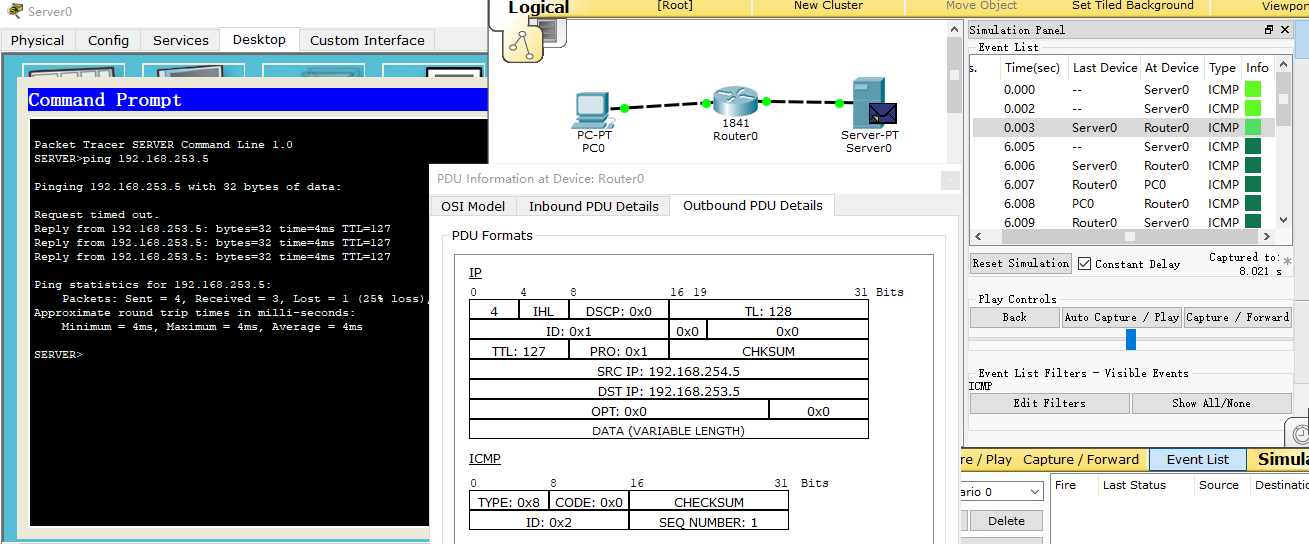
简介：

ICMP报文包含在IP数据报中，属于IP的一个用户，IP头部就在ICMP报文的前面，所以一个ICMP报文包括IP头部、ICMP头部和ICMP报文，IP头部的Protocol值为1就说明这是一个ICMP报文，ICMP头部中的类型（Type）域用于说明ICMP报文的作用及格式，此外还有一个代码（Code）域用于详细说明某种ICMP报文的类型，所有数据都在ICMP头部后面。





C:\Users\Administrator\AppData\Roaming\Tencent\Users\5651643\QQ\WinTemp\RichOle\TKQ$LPC)M2SNI1W213Q~`(C.png



Wireshark可以捕获和显示通过网络接口进出其所在PC的所有网络通信。Packet Tracer的模拟模式可以捕获流经整个网络的所有网络通信，但支持的协议数量有限。我们使用的网络中包含一台通过路由器连接到服务器的PC，并且可以捕获从PC发出的ping命令的输出。

任务1：使用Packet Tracer捕获和研究ICMP报文。

**步骤1.捕获并评估到达Eagle Server的ICMP回应报文。**

进入Simulation（模拟）模式。Event List Filters（事件列表过滤器）设置为只显示ICMP事件。单击Pod PC。从Desktop（桌面）打开Command Prompt（命令提示符）。输入命令ping eagle-server.example.com并按Enter键。最小化Pod PC配置窗口。单击Auto Capture/Play（自动捕获/播放）按钮以运行模拟和捕获事件。收到"No More Events"（没有更多事件）消息时单击OK（确定）。

在Event List（事件列表）中找到第一个数据包，即第一条回应请求，然后单击Info（信息）列中的彩色正方形。单击事件列表中数据包的Info（信息）正方形时，将会打开PDU Information（PDU信息）窗口。单击Outbound PDU Details（出站PDU详细数据）选项卡以查看ICMP报文的内容。请注意，Packet Tracer只显示TYPE（类型）和CODE（代码）字段。

要模拟Wireshark的运行，请在其中At Device（在设备）显示为Pod PC的下一个事件中，单击其彩色正方形。这是第一条应答。单击Inbound PDU Details（入站PDU详细数据）选项卡以查看ICMP报文的内容。

查看At Device（在设备）为Pod PC的其余事件。完成时单击Reset Simulation（重置模拟）按钮。

**步骤2.捕获并评估到达192.168.253.1的ICMP回应报文。**

使用IP地址192.168.253.1重复步骤1。观看动画，注意哪些设备参与交换。

**步骤3.捕获并评估超过TTL值的ICMP回应报文。**

Packet Tracer不支持ping -i选项。在模拟模式中，可以使用Add Complex PDU（添加复杂 PDU）按钮（开口的信封）设置TTL。

单击Add Complex PDU（添加复杂 PDU）按钮，然后单击Pod PC（源）。将会打开Create Complex PDU（创建复杂 PDU）对话框。在Destination IP Address:（目的 IP 地址：）字段中输入192.168.254.254。将TTL:字段中的值改为1。在Sequence Number（序列号）字段中输入1。在Simulation Settings（模拟设置）下选择Periodic（定期） 选项。在Interval（时间间隔）字段中输入2。单击Create PDU（创建PDU）按钮。此操作等同于从Pod PC上的命令提示符窗口发出命令ping -t -i 1 192.168.254.254。

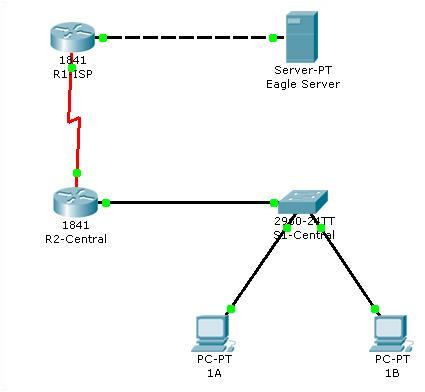
重复单击Capture/Forward（捕获/转发）按钮，以在Pod PC与路由器之间生成多次交换。

在Event List（事件列表）中找到第一个数据包，即第一个回应请求。然后单击Info（信息）列中的彩色正方形。单击事件列表中数据包的Info（信息）正方形时，将会打开PDU Information（PDU信息）窗口。单击Outbound PDU Details（出站PDU详细数据）选项卡以查看ICMP报文的内容。

要模拟Wireshark的运行，请在其中At Device（在设备）为Pod PC的下一个事件中，单击其彩色正方形。这是第一条应答。单击Inbound PDU Details（入站PDU详细数据）选项卡以查看ICMP报文的内容。  
查看At Device（在设备）为Pod PC的其余事件。

## 实验6、地址解析协议(ARP)

**拓扑图如下：**



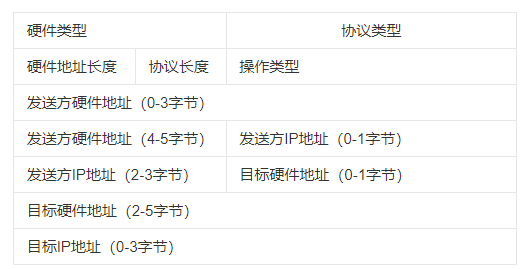
学习目标

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。



硬件类型：指明了发送方想知道的硬件接口类型，以太网的值为1；

协议类型：指明了发送方提供的高层协议类型，IP为0800（16进制）；

硬件地址长度和协议长度：指明了硬件地址和高层协议地址的长度，这样ARP报文就可以在任意硬件和任意协议的网络中使用；

操作类型：用来表示这个报文的类型，ARP请求为1，ARP响应为2，RARP请求为3，RARP响应为4；

发送方硬件地址（0-3字节）：源主机硬件地址的前3个字节；

发送方硬件地址（4-5字节）：源主机硬件地址的后3个字节；

发送方IP地址（0-1字节）：源主机IP地址的前2个字节；

发送方IP地址（2-3字节）：源主机IP地址的后2个字节；

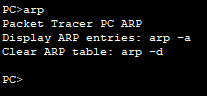
目标硬件地址（0-1字节）：目的主机硬件地址的前2个字节；

目标硬件地址（2-5字节）：目的主机硬件地址的后4个字节；

目标IP地址（0-3字节）：目的主机的IP地址。

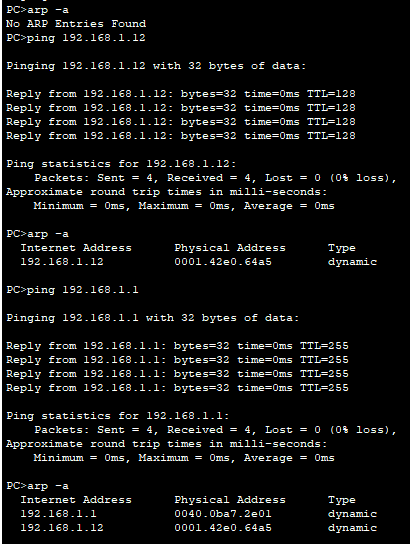
**任务1：使用Packet Tracer的arp命令**

步骤1.访问命令提示符窗口。单击PC1A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PC1A上ping地址192.168.1.12，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。

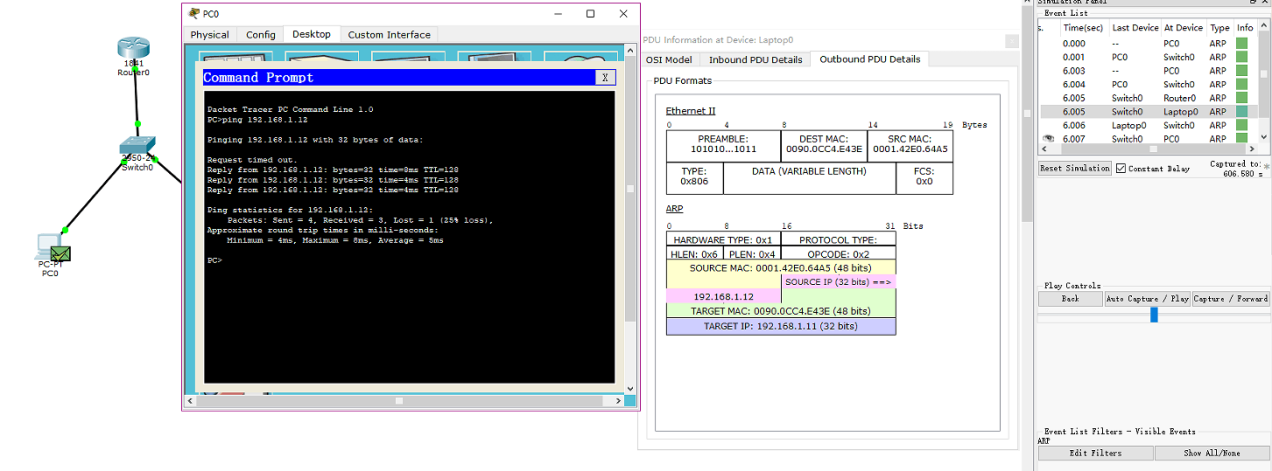
进入模拟模式。确认Event List Filters（事件列表过滤器）只显示ARP事件。

步骤2.准备Pod主机以执行ARP捕获。

在PC1A上使用Packet Tracer命令arp -d。然后Ping地址 192.168.1.12。

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。



开始研究本节课的拓扑图吧！