**协议报文分析实验**

**实验2 协议报文分析**

**学习目标**

* 掌握以太网帧结构
* 掌握IP报文结构
* 掌握TCP/UDP报文结构
* 掌握ICMP报文结构，熟练使用ping 和tracert命令
* 掌握ARP协议原理及工作过程

**拓扑图**

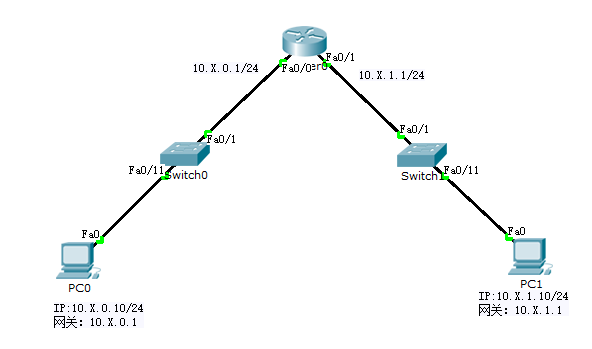


图1 协议报文分析拓扑

**操作步骤**

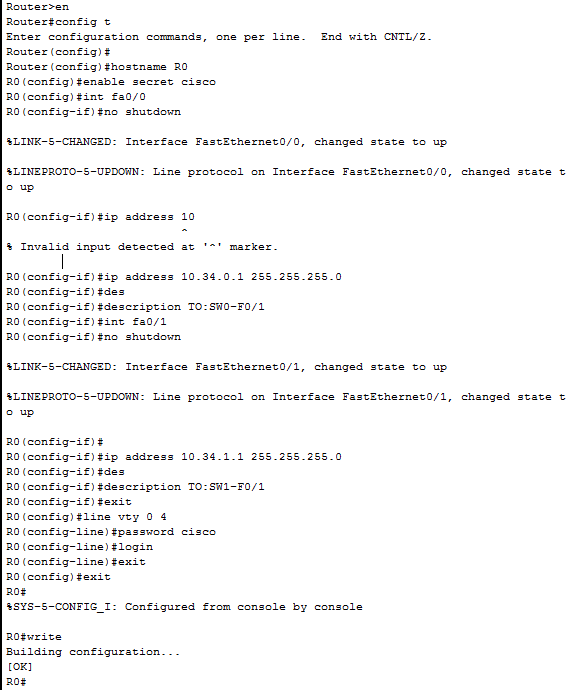
1. **配置各设备基础配置**

按照拓扑图组网，并完成基础配置：

R0:

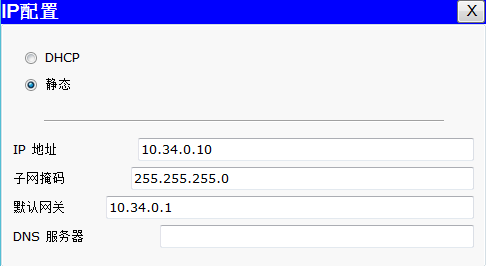
|  |
| --- |
| *Router>EN*  *Router#conf*  *Configuring from terminal, memory, or network [terminal]?*  *Enter configuration commands, one per line. End with CNTL/Z.*  *Router(config)#hostname R0 //设置设备名称*  *R0(config)#int f0/0 //进入F0/0接口*  *R0(config-if)#no shutdown //开启接口*  *R0(config-if)#ip add 10.X.0.1 255.255.255.0 //配置IP地址，注意X表示学号*  *R0(config-if)#description TO:SW0-F0/1 //接口描述*  *R0(config)#int f0/1*  *R0(config-if)#no shutdown*  *R0(config-if)#ip add 10.X.1.1 255.255.255.0 //配置IP地址，注意X表示学号*  *R0(config-if)#description TO:SW1-F0/1*  *R0(config-if)#exit*  *R0(config)#line vty 0 4*  *R0(config-line)#password cisco //配置telnet密码为cisco*  *R0(config-line)#login //配置密码认证*  *R0(config-line)#exit*  *R0(config)#exit*  *R0#*  *%SYS-5-CONFIG\_I: Configured from console by console*  *R0#wr*  *Building configuration...*  *[OK]*  *R0#* |

操作截图如下：

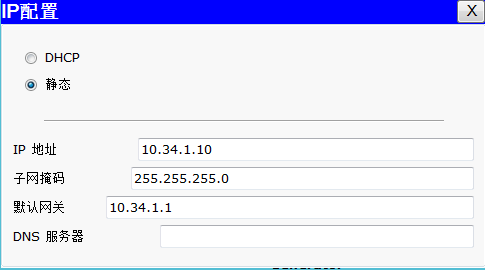


SW0 和SW1 不用进行配置

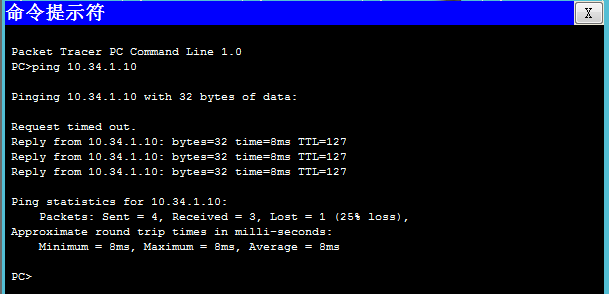
PC0 //注意根据个人学号配置IP地址和网关，此处以“34”为例。



PC1 //注意根据个人学号配置IP地址和网关，此处以“34”为例。

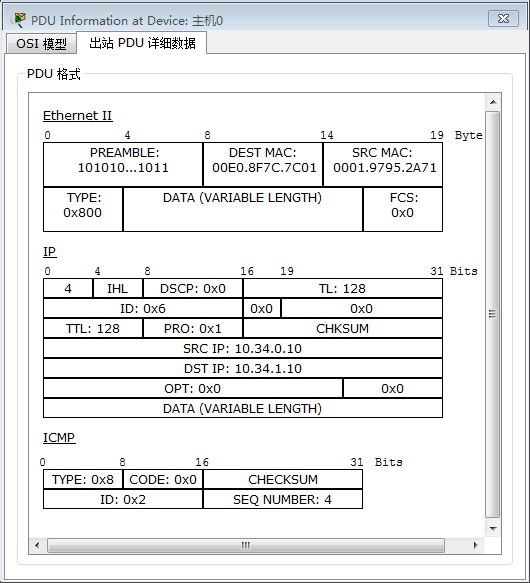


1. **Ping命令使用和报文分析**
2. 单击右下角“模拟”图标；
3. 单击“自动捕获/播放”；
4. 在PC0“命令提示符”中进行ping测试。

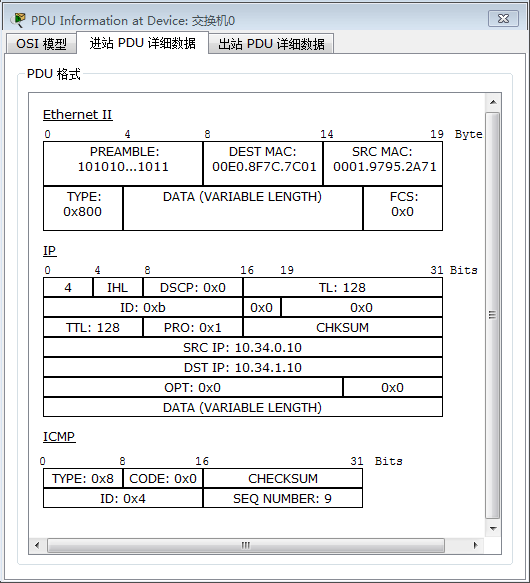


1. 查看“事件列表”中报文交互情况。
2. 选择“ICMP”报文，进行报文分析。





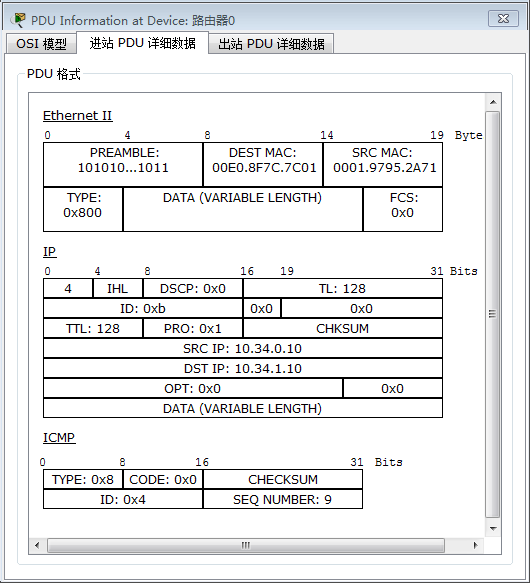
1. 请回答如下问题：
2. 请找出PC0发送至SW0设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？



答：由上图，源MAC：0001.9795.2A71 目的MAC：00E0.8F7C.7C01

源IP：10.34.0.10 目的IP：10.34.1.10

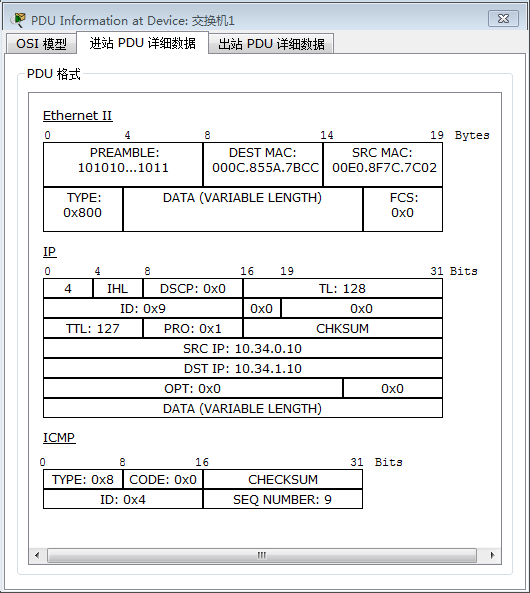
1. 请找出SW0发送至R0设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？



答：由上图，源MAC：0001.9795.2A71 目的MAC：00E0.8F7C.7C01

源IP：10.34.0.10 目的IP：10.34.1.10

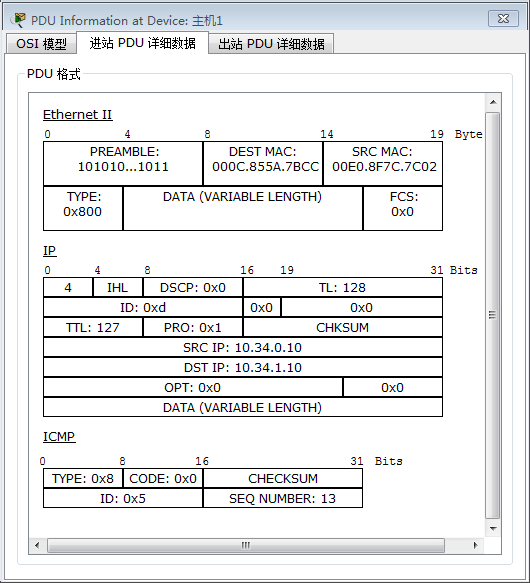
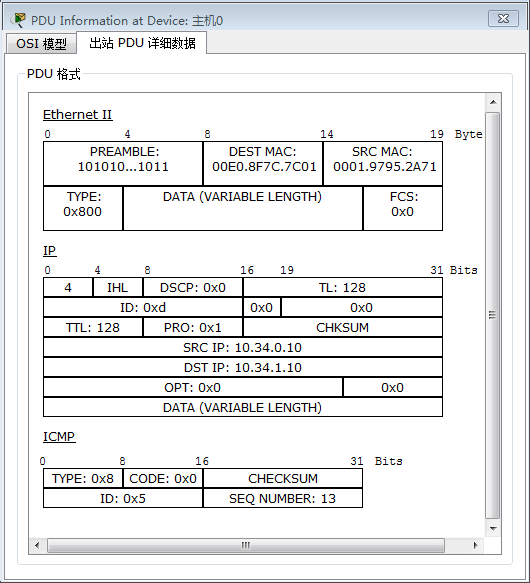
1. 请找出R0发送至SW1设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？



答：由上图，源MAC：00E0.8F7C.7C02 目的MAC：000C.855A.7BCC

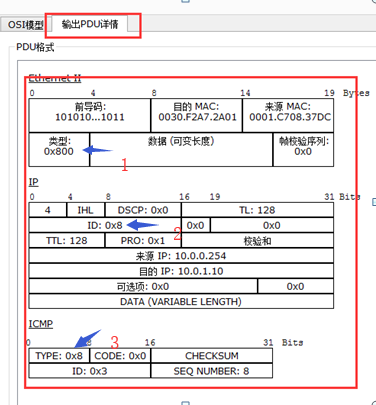
源IP：10.34.0.10 目的IP：10.34.1.10

1. 从PC0发出的报文的IP头部，在发送至PC1时哪些内容发生了变化？



答：由上两图比较可知，PC0发出的报文的IP头部，在发送至PC1时,TTL递减了1。

1. 如下图所标注，各字段的含义是什么？

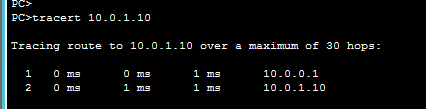


答：由上图比较可知，标号1表示协议类型，封装了IP协议；

标号2表示IP报文的标识为0x8，主机每发一个报文，加1，分片重组时会用到该字段；

标识3表示消息类型，值为0x8，此报文为请求回显报文。

1. **Tracert 命令使用和报文分析**
2. 在PC0“命令提示符”中进行tracert测试。



1. 查看“事件列表”中报文交互情况。
2. 请回答如下问题：
3. tracert 有什么作用？

答：tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP数据包访问目标所采取的路径。tracert 命令使用用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由.

1. tracert 的工作原理？

答：通过向目标发送不同 IP 生存时间 (TTL) 值的“Internet 控制消息协议 (ICMP)”回应数据包，tracert诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。

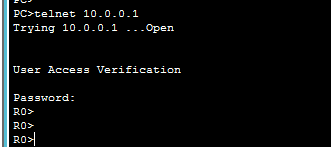
1. PC0发出的报文有何规律？

答：PC0发出的报文里TTL值为1，这说明tracert 先发送 TTL 为 1 的回应数据包，并随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。

1. **telnet 协议交互过程**
2. 执行在PC0“命令提示符”中进行telnet R0。



1. 单击“模拟”，查看“事件列表”中报文交互情况。
2. 在PC0上输入密码“cisco”，后回车，登录R0成功。



1. 查看“事件列表”中报文交互情况。
2. 交互完成后，在PC0上，退出R0。
3. 查看“事件列表”中报文交互情况。
4. 请回答如下问题：
5. 寻找到TCP建立过程中三次握手的报文并截图。



1. 为什么TCP建立连接使用三次握手，断开连接使用四次握手？

答：为了应对网络中存在的延迟的重复数组的问题 (已失效的连接请求报文段)，TCP 需要 seq 序列号来做可靠重传或接收，而避免连接复用时无法分辨出seq 是延迟或者是旧链接的seq，因此需要三次握手来约定确定双方的 ISN（初始 seq 序列号）；因为TCP连接是全双工的网络协议，允许同时通信的双方同时进行数据的收发，同样也允许收发两个方向的连接被独立关闭，以避免client数据发送完毕，向server发送FIN关闭连接，而server还有发送到client的数据没有发送完毕的情况。所以关闭TCP连接需要进行四次握手，每次关闭一个方向上的连接需要FIN和ACK两次握手。

1. telnet协议有何作用，是由什么协议承载的，端口号是多少？

答：Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议。Telnet协议的目的是提供一个相对通用的，双向的，面向八位字节的通信方法，允许界面终端设备和面向终端的过程能通过一个标准过程进行互相交互，应用Telnet协议能够把本地用户所使用的计算机变成远程主机系统的一个终端。

端口号是23。

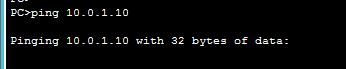
1. **ARP协议及交互过程。**
2. 在PC0上查看ARP表项，使用命令“arp -a”；



1. 如果PC0上有arp信息，可使用命令“arp -d”删除。



1. 单击“模拟”，在PC0上ping 10.0.1.10；



1. 在“事件列表中”查看ARP交互过程。
2. 请回答如下问题：
3. 什么情况下会进行ARP？

答：主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。

1. ARP协议的作用是什么？

答：ARP（地址解析协议）是根据IP地址获取物理地址的一个TCP/IP协议。

1. ARP的请求和回应报文各是单播、组播还是广播报文？

答：ARP的请求报文是广播报文，回应报文是单播报文。