



湖南大学  
HUNAN UNIVERSITY

# 课程实验报告

课 程 名 称: 计算机网络  
实验项目名称: 实验五  
专 业 班 级: 计科 1702  
姓 名: 姚成伟  
学 号: 201708010205  
完 成 时 间: 2020 年 5 月 17 日

信息科学与工程学院

## 一、实验目的：

通过本实验，进一步熟悉 PacketTracer 的使用，学习路由器与交换机的基本配置，加深对网络层与链路层协议的理解。

## 二、实验内容：

### 4.1 路由器交换机的基本配置

打开下面的实验文件，按提示完成实验。



### 4.2 了解 ICMP 数据包的格式

使用 Packet Tracer 捕获并研究 ICMP 报文

使用的网络中包含一台通过路由器连接到服务器的 PC，并且捕获从 PC 发出的 ping 命令的输出。

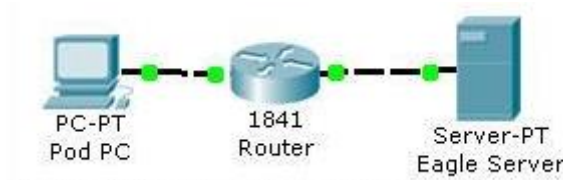


图 4.1 捕获 ICMP 报文

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 (进站 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 (进站 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。

### 4.3 检查 ARP 交换

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。

在此任务结束时，完成率应为 100%。

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。

### 三、实验步骤：

#### 任务 1：路由器交换机的基本配置：

##### 1、路由器的基本配置：

## 实验：路由器的一些基本配置



2811  
路由器0

```
R1>show version
此命令结果包含有IOS版本，IOS映像文件，
存储器大小，接口类型及配置登记值等信息。

Router>enable
Router#configure terminal
Router(config)#hostname R1

R1(config)#no ip domain-lookup
关闭域名解释

R1(config)#line console 0
R1(config-line)#logging synchronous
设置输入同步

R1(config-line)#exec-timeout 20 00
设置执行会话时间
R1(config-line)#end
```

按照提示进行配置：

```
Router>show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12
1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 20 00
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

## 2、静态路由：

**Logical** [Root]

实验：静态路由

静态路由配置是网络配置中最主要、最基本的配置。静态路由配置是指网络管理员手动配置路由表，指定数据包从源地址到目的地址的路径。静态路由配置适用于小型网络或网络边缘，配置简单，易于管理。

静态路由配置的基本命令如下：

```
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.2
```

其中，192.168.1.0 255.255.255.0 是目的网络的地址和子网掩码，192.168.1.2 是下一跳的IP地址。

静态路由配置的优点如下：

- (1) 配置简单：静态路由配置只需要配置目的网络的地址和子网掩码以及下一跳的IP地址即可。
- (2) 易于管理：静态路由配置不需要配置路由协议，因此配置简单，易于管理。
- (3) 安全性高：静态路由配置不需要配置路由协议，因此配置简单，易于管理。

静态路由配置的缺点如下：

- (1) 配置复杂：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。
- (2) 易于管理：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。
- (3) 安全性高：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。

静态路由配置的基本命令如下：

```
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.2
```

其中，192.168.1.0 255.255.255.0 是目的网络的地址和子网掩码，192.168.1.2 是下一跳的IP地址。

静态路由配置的优点如下：

- (1) 配置简单：静态路由配置只需要配置目的网络的地址和子网掩码以及下一跳的IP地址即可。
- (2) 易于管理：静态路由配置不需要配置路由协议，因此配置简单，易于管理。
- (3) 安全性高：静态路由配置不需要配置路由协议，因此配置简单，易于管理。

静态路由配置的缺点如下：

- (1) 配置复杂：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。
- (2) 易于管理：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。
- (3) 安全性高：静态路由配置需要配置目的网络的地址和子网掩码以及下一跳的IP地址，配置相对复杂。

按照提示操作：

路由器转发数据包时需要查找路由表，管理员可以通过手工的方法在路由器中直接配置路由表，这就是静态路由。静态路由的缺点是不能动态反映网络拓扑，当网络拓扑发生变化时，管理员就必须手工改变路由表；然而静态路由不会占用路由器太多的 CPU 和 RAM 资源，也不占用线路的带宽。配置静态路由的命令为“ip route”，命令的格式如下：

ip route 目的网络 掩码 { 网关地址 | 接口 }

例子：ip route 192.168.1.0 255.255.255.0 s0/0

例子：ip route 192.168.1.0 255.255.255.0 12.12.12.2

在写静态路由时，如果链路是点到点的链路（例如 PPP 封装的链路），采用网关地址和接口都是可以的；然而如果链路是多路访问的链路（例如以太网），则只能采用网关地址即不能：ip route 192.168.1.0 255.255.255.0 f0/0。

配置信息如下：

R1：（拓扑图中其实是 R0）

```
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#int loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#int s2/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000
R1(config-if)#ip route 2.2.2.0 255.255.255.0 s2/0
R1(config)#ip route 3.3.3.0 255.255.255.0 192.168.1.2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

R1 的路由表如下：

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
    2.0.0.0/24 is subnetted, 1 subnets
S       2.2.2.0 is directly connected, Serial2/0
    3.0.0.0/24 is subnetted, 1 subnets
S       3.3.3.0 [1/0] via 192.168.1.2
C     192.168.1.0/24 is directly connected, Serial2/0
```

ping 命令测试

```

R1#ping
Protocol [ip]:
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/103/492 ms

```

R2:

```

R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2
R2(config)#int loopback0
R2(config-if)#ip address 2.2.2.2 255.255.255.0
R2(config-if)#exit
R2(config)#int s2/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int s3/0
R2(config-if)#ip address 192.168.100.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#clock rate 64000
R2(config-if)#ip route 1.1.1.0 255.255.255.0 s2/0
R2(config)#ip route 3.3.3.0 255.255.255.0 s3/0
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

```

查看路由表:

```

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 1 subnets
S       1.1.1.0 is directly connected, Serial2/0
    2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
    3.0.0.0/24 is subnetted, 1 subnets
S       3.3.3.0 is directly connected, Serial3/0
C       192.168.1.0/24 is directly connected, Serial2/0
C       192.168.100.0/24 is directly connected, Serial3/0

```

R3:

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int loopback0
R3(config-if)#ip address 3.3.3.3 255.255.255.0
R3(config-if)#exit
R3(config)#int s2/0
R3(config-if)#ip address 192.168.100.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 1.1.1.0 255.255.255.0 s2/0
R3(config)#ip route 2.2.2.0 255.255.255.0 s2/0
R3(config)#

```

路由表:

```

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 1 subnets
S       1.1.1.0 is directly connected, Serial2/0
    2.0.0.0/24 is subnetted, 1 subnets
S       2.2.2.0 is directly connected, Serial2/0
    3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Loopback0
C    192.168.100.0/24 is directly connected, Serial2/0
R3#

```

### 3、子网划分:

**实验：子网划分**

划分子网的一些公式：

- 你所选择的子网掩码将会产生多少个子网：  
2的x次方（x代表被借走的主机位数）。
- 每个子网有多少主机：2的y次方-2（y代表被借走之后剩余的主机位数）。
- 有效子网是：有效子网号=256-十进制的子网掩码（结果叫做block size）。
- 每个子网的广播地址是：广播地址=下一个子网号-1
- 每个子网的有效主机分别是：忽略子网内全为0和全为1的地址剩下的就是有效主机地址。  
网络地址192.168.10.0 子网掩码255.255.255.192

1. 子网数=2的2次方=4。

2. 每个子网的主机数=2的6次方-2=62。

3. 有效子网：block size=256-192=64，第一个子网为192.168.10.0，第二个子网为192.168.10.64，第三个子网为192.168.10.128，最后一个为192.168.10.192。

4. 广播地址：下一个子网-1，第一个子网的广播地址是192.168.10.63，第二个是192.168.10.127，第三个是192.168.10.191，最后一个为192.168.10.255。

5. 有效主机范围是：第一个子网的主机地址是192.168.10.1到192.168.10.62，第二个是192.168.10.65到192.168.10.126，第三个是192.168.10.129到192.168.10.190，最后一个为192.168.10.193到192.168.10.254。



划分子网的一些公式：

1. 你所选择的子网掩码将会产生多少个子网：2 的 x 次方 (x 代表被借走的主机位数)。

2. 每个子网有多少主机：2 的 y 次方 - 2 (y 代表被借走之后剩余的主机位数)。

3. 有效子网是：有效子网号 = 256 - 十进制的子网掩码 (结果叫做 block size)。

4. 每个子网的广播地址是：广播地址 = 下一个子网号 - 1

5. 每个子网的有效主机分别是：忽略子网内全为 0 和全为 1 的地址剩下的就是有效主机地址。最后有效的 1 个主机地址 = 下一个子网号 - 2 (即广播地址 - 1)

如图：网络地址 192.168.10.0，子网掩码 255.255.255.192

1. 子网数 = 2 的 2 次方 = 4。


2. 每个子网的主机数 = 2 的 6 次方 - 2 = 62。

3. 有效子网：block size = 256 - 192 = 64，第一个子网为 192.168.10.0，第二个子网为 192.168.10.64，第三个子网为 192.168.10.128，最后一个为 192.168.10.192。

4. 广播地址：下一个子网 - 1，第一个子网的广播地址是 192.168.10.63，第二个是 192.168.10.127，第三个是 192.168.10.191，最后一个为 192.168.10.255。

5. 有效主机范围是：第一个子网的主机地址是 192.168.10.1 到 192.168.10.62，第二个是 192.168.10.65 到 192.168.10.126，第三个是 192.168.10.129 到 192.168.10.190，最后一个为 192.168.10.193 到 192.168.10.254。

#### 4、配置 RIP：



实验：配置RIP

```
R1#show ip protocols
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#end
R1#show ip route
R1#clear ip route *
R1#show ip route

R2(config)#router rip
R2(config-router)#network 192.168.1.0
R2(config-router)#network 172.16.0.0
R2(config-router)#end
R2#show ip route
R2#clear ip route *
R2#show ip route

R3(config)#router rip
R3(config-router)#network 172.16.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#end
R3#show ip route

R4(config)#router rip
R4(config-router)#network 10.0.0.0
R4(config-router)#end
R4#show ip protocols
R4#show ip route
```

路由器13: 2811, 192.168.1.1, 255.255.255.0  
路由器14: 2811, 192.168.1.2, 255.255.255.0  
路由器15: 2811, 172.16.1.1, 255.255.0.0  
路由器16: 2811, 10.1.1.1, 255.0.0.0

路由选择信息协议 (RIP/RIP2/RIPng: Routing Information Protocol)

路由协议	默认管理距离
直连网络	0
静态路由	1
EIGRP (internal)	90
IGRP	100
OSPF	110
RIPv1/RIPv2	120

管理距离越小，可信度越高，优先采用可信度高的路由协议。

R1:

```
R1>enable
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  FastEthernet0/0      1    2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.1.2      120          00:00:20
Distance: (default is 120)
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

路由表:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/2] via 192.168.1.2, 00:00:05, FastEthernet0/0
R    172.16.0.0/16 [120/1] via 192.168.1.2, 00:00:05, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

```
R1#clear ip route *
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

R2:

```

R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 192.168.1.0
R2(config-router)#network 172.16.0.0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

```

路由表:

```

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 172.16.1.2, 00:00:28, FastEthernet0/1
C    172.16.0.0/16 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R2#

```

```

R2#clear ip route *
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.16.0.0/16 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R2#

```

R3:

```

R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 172.16.0.0
R3(config-router)#network 10.0.0.0
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

```

路由表:

```

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 172.16.1.1, 00:00:23, FastEthernet0/0
R3#

```

R4:

```

R4>enable
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router rip
R4(config-router)#network 10.0.0.0
R4(config-router)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console

```

路由协议:

```

R4#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  FastEthernet0/0      1    2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.1.1         120           00:00:12
Distance: (default is 120)

```

路由表:

```

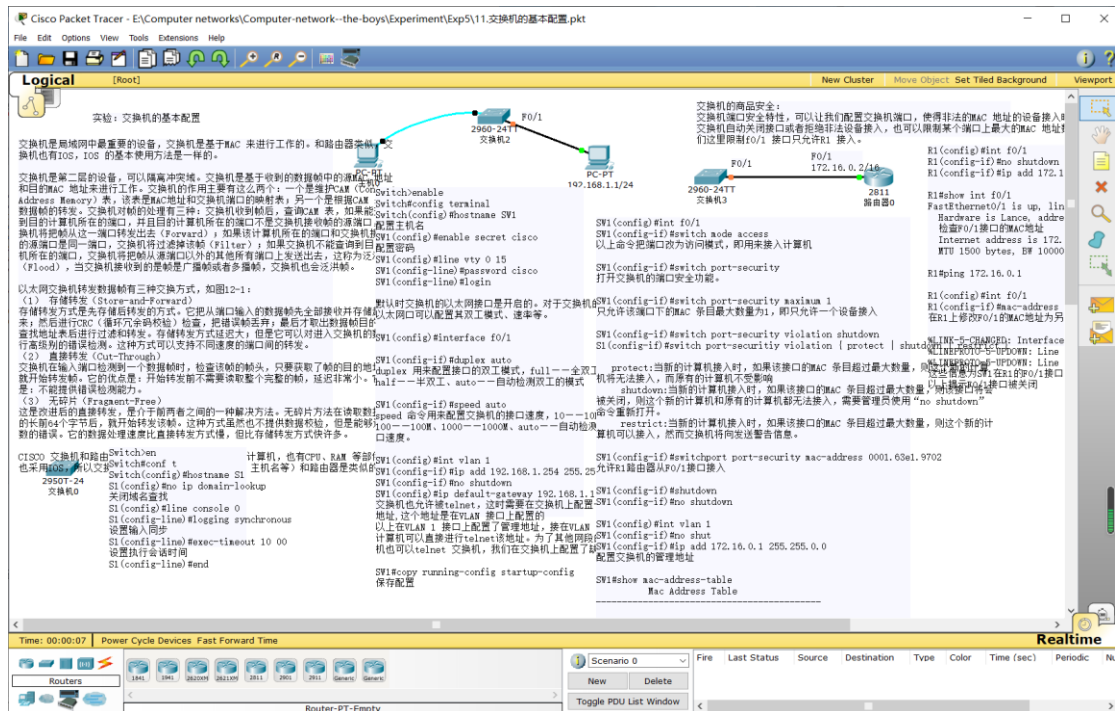
R4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
R    172.16.0.0/16 [120/1] via 10.1.1.1, 00:00:02, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 10.1.1.1, 00:00:02, FastEthernet0/0
R4#

```

## 5、交换机基本配置



交换机是局域网中最重要的设备，交换机是基于 MAC 来进行工作的。和路由器类似，交换机也有 IOS，IOS 的基本使用方法是一样的。

交换机是第二层的设备，可以隔离冲突域。交换机是基于收到的数据帧中的源 MAC 地址和目的 MAC 地址来进行工作。交换机的作用主要有这么两个：一个是维护 CAM (ContextAddress Memory) 表，该表是 MAC 地址和交换机端口的映射表；另一个是根据 CAM 来进行数据帧的转发。交换机对帧的处理有三种：交换机收到帧后，查询 CAM 表，如果能查询到目的计算机所在的端口，并且目的计算机所在的端口不是交换机接收帧的源端口，交换机将把帧从这一端口转发出去 (Forward)；如果该计算机所在的端口和交换机接收帧的源端口是同一端口，交换机将过滤掉该帧 (Filter)；如果交换机不能查询到目的计算机所在的端口，交换机将把帧从源端口以外的其他所有端口上发送出去，这称为泛洪 (Flood)，当交换机接收到的是帧是广播帧或者多播帧，交换机也会泛洪帧。

以太网交换机转发数据帧有三种交换方式。

### (1) 存储转发 (Store-and-Forward)

存储转发方式是先存储后转发的方式。它把从端口输入的数据帧先全部接收并存储起来；然后进行 CRC (循环冗余码校验) 检查，把错误帧丢弃；最后才取出数据帧目的地址，查找地址表后进行过滤和转发。存储转发方式延迟大；但是它可以对进入交换机的数据包进行高级别的错误检测。这种方式可以支持不同速度的端口间的转发。

## (2) 直接转发 (Cut-Through)

交换机在输入端口检测到一个数据帧时，检查该帧的帧头，只要获取了帧的目的地地址，就开始转发帧。它的优点是：开始转发前不需要读取整个完整的帧，延迟非常小。它的缺点是：不能提供错误检测能力。

## (3) 无碎片 (Fragment-Free)

这是改进后的直接转发介于前两者之间的一种解决方法。无碎片法在读取数据帧的长前 64 个字节后就开始转发该帧。这种方式虽然不提供数据校验，但是能够避免多数的错误。它的数据处理速度比直接转发方式慢，但比存储转发方式快许多。CISCO 交换机和路由器一样，本质上也是一台特殊的计算机，也有 CPU、RAM 等部件。也采用 IOS，所以交换机的很多基本配置（例如密码、主机名等）和路由器是类似的。

交换机基本配置：

```
S1>enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#logging synchronous
S1(config-line)#exec-timeout 10 00
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

交换机 SW1 配置：

```
SW1>enable
Password:
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#enable secret cisco
SW1(config)#line vty 0 15
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#int f0/1
SW1(config-if)#duplex auto
SW1(config-if)#speed auto
SW1(config-if)#exit
SW1(config)#int vlan 1
SW1(config-if)#ip add 192.168.1.254 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#ip default-gateway 192.168.1.100
SW1(config)#exit
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW1#
```

默认时交换机的以太网接口是开启的。对于交换机的以太网口可以配置其双工模式、速率等。duplex 用来配置接口的双工模式，full—全双工、half—半双工、auto—自动检



测双工的模式。speed 命令用来配置交换机的接口速度, 10—10M、100—100M、1000—1000M、auto—自动检测接口速度。

交换机也允许被 telnet, 这时需要在交换机上配置一个 IP 地址,这个地址是在 VLAN 接口上配置的以上在 VLAN 1 接口上配置了管理地址, 接在 VLAN 1 上的计算机可以直接进行 telnet 该地址。为了其他网段的计算机也可以 telnet 交换机, 我们在交换机上配置了缺省网关。

SW1 的安全配置:

```
SW1>enable
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#int f0/1
SW1(config-if)#switch mode access
SW1(config-if)#switch port-security
SW1(config-if)#switch port-security maximum 1
SW1(config-if)#switch port-security maximum 1 violation shutdown
^
% Invalid input detected at '^' marker.
SW1(config-if)#switch port-security violation shutdown
```

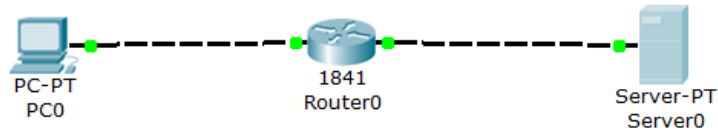
交换机端口安全特性, 可以让我们配置交换机端口, 使得非法的 MAC 地址的设备接入时, 交换机自动关闭接口或者拒绝非法设备接入, 也可以限制某个端口上最大的 MAC 地址数。我们这里限制 f0/1 接口只允许 R1 接入。

使用命令把端口改为访问模式, 即用来接入计算机。

在命令: S1(config-if)#switch port-security violation { protect | shutdown | restrict }中, protect: 当新的计算机接入时, 如果该接口的 MAC 条目超过最大数量, 则这个新的计算机将无法接入, 而原有的计算机不受影响; shutdown: 当新的计算机接入时, 如果该接口的 MAC 条目超过最大数量, 则该接口将会被关闭, 则这个新的计算机和原有的计算机都无法接入, 需要管理员使用“no shutdown”命令重新打开; restrict: 当新的计算机接入时, 如果该接口的 MAC 条目超过最大数量, 则这个新的计算机可以接入, 然而交换机将向发送警告信息。

## 任务 2: 了解 ICMP 数据包的格式

实验拓扑图:



PC0 的配置:

**IP Configuration**

IP Configuration  
☐ DHCP ☒ Static

IP Address: 172.16.1.1  
Subnet Mask: 255.255.0.0  
Default Gateway: 172.16.255.254  
DNS Server: 172.16.254.254

IPv6 Configuration  
☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /  
Link Local Address: FE80::20A:41FF:FE76:3881  
IPv6 Gateway:

Web Browser  
Cisco IP Communicator

路由器 R0 的配置:

F0/0 端口:

**Router0**

Physical Config CLI

**GLOBAL**

Settings  
Algorithm Settings

**ROUTING**

Static  
RIP

**SWITCHING**

VLAN Database

**INTERFACE**

FastEthernet0/0  
FastEthernet0/1

**FastEthernet0/0**

Port Status ☒ On  
Bandwidth ☒ Auto  
☐ 10 Mbps ☒ 100 Mbps  
Duplex ☒ Auto  
☐ Full Duplex ☒ Half Duplex  
MAC Address: 00E0.F97A.9401  
IP Address: 172.16.255.254  
Subnet Mask: 255.255.0.0  
Tx Ring Limit: 10

Equivalent IOS Commands

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
to up
```



F0/1 端口：

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar shows a tree view with 'FastEthernet0/1' selected under the 'INTERFACE' section. The main area displays the configuration for 'FastEthernet0/1'.

FastEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps	
Duplex	<input checked="" type="checkbox"/> Auto
<input type="radio"/> Full Duplex <input checked="" type="radio"/> Half Duplex	
MAC Address	00E0.F97A.9402
IP Address	192.168.254.253
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Equivalent IOS Commands

```
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed  
o up
```

记得要打开两个端口。

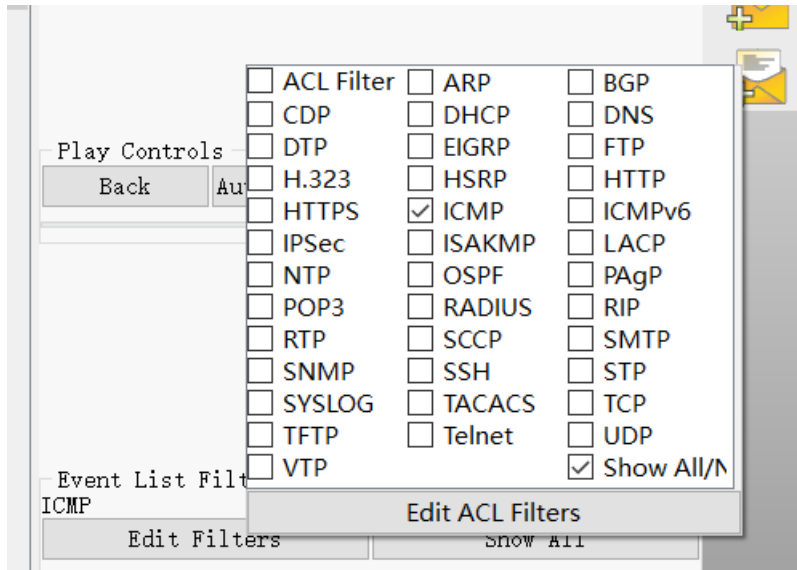
服务器配置：

The screenshot shows the 'Server0' configuration window with the 'Config' tab selected. The 'IP Configuration' window is open, showing settings for 'FastEthernet0'.

IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	192.168.254.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.254.253
DNS Server	
IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::204:9AFF:FE8E:1DAE

Web Browser

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。

```
PC>ping 192.168.254.254
```

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）。

Time(s)	Last Dev	Ac Dev	Type	Info
1959....	--	PC0	IC...	
1959....	PC0	Router0	IC...	
1959....	Router0	Server0	IC...	
1959....	Server0	Router0	IC...	
1959....	Router0	PC0	IC...	

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。

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19 bytes
PREAMBLE: 101010...1011		DEST MAC: 00E0.F97A.94	SRC MAC: 000A.4176.38	
TYPE: 0x800	DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 128		
ID: 0xe		0x0	0x0		
TTL: 128	PRO: 0x1	CHKSUM			
SRC IP: 172.16.1.1					
DST IP: 192.168.254.254					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31 Bits
TYPE:	CODE:	CHECKSUM	
ID: 0x2		SEQ NUMBER: 2	

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（进站 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。

PDU Information at Device: PC0

OSI Model

Inbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	bytes
PREAMBLE: 101010...1011		DEST MAC: 000A.4176.38		SRC MAC: 00E0.F97A.94	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0		TL: 128		
ID: 0x1		0x0		0x0		
TTL: 127		PRO: 0x1		CHKSUM		
SRC IP: 192.168.254.254						
DST IP: 172.16.1.1						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits	
TYPE:		CODE:		CHECKSUM	
ID: 0x2		SEQ NUMBER: 2			

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。

```
PC>ping 192.168.253.1

Pinging 192.168.253.1 with 32 bytes of data:

Reply from 172.16.255.254: Destination host unreachable.
Reply from 172.16.255.254: Destination host unreachable.
```

Vis.	Time(s)	Last Dev	At Devi	Type	Info
	0.000	--	PC0	IC...	
	0.001	PC0	Router0	IC...	
	0.001	--	Router0	IC...	
	0.002	Router0	PC0	IC...	
	1.004	--	PC0	IC...	
	1.005	PC0	Router0	IC...	
	1.005	--	Router0	IC...	

只有 PC0 和 R0 参与了交换。

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	ytes
PREAMBLE: 101010...1011		DEST MAC: 00E0.F97A.94		SRC MAC: 000A.4176.38	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0		TL: 128		
ID: 0x12		0x0		0x0		
TTL: 128		PRO: 0x1		CHKSUM		
SRC IP: 172.16.1.1						
DST IP: 192.168.253.1						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE:		CODE:		CHECKSUM
ID: 0x4		SEQ NUMBER: 6		

PDU Information at Device: PC0

OSI Model Inbound PDU Details

PDU Formats

4	IHL	DSCP: 0x0	TL: 156
ID: 0x1	0x0	0x0	
TTL: 255	PRO: 0x1	CHKSUM	
SRC IP: 172.16.255.254			
DST IP: 172.16.1.1			
OPT: 0x0		0x0	
DATA (VARIABLE LENGTH)			

ICMP

0 8 16 31 Bits			
TYPE:	CODE:	CHECKSUM	
ID: 0x4	SEQ NUMBER: 0		

IP

0 4 8 16 19 31 Bits			
4	IHL	DSCP: 0x0	TL: 128
ID: 0x12	0x0	0x0	
TTL: 128	PRO: 0x1	CHKSUM	
SRC IP: 172.16.1.1			
DST IP: 192.168.253.1			
OPT: 0x0		0x0	
DATA (VARIABLE LENGTH)			

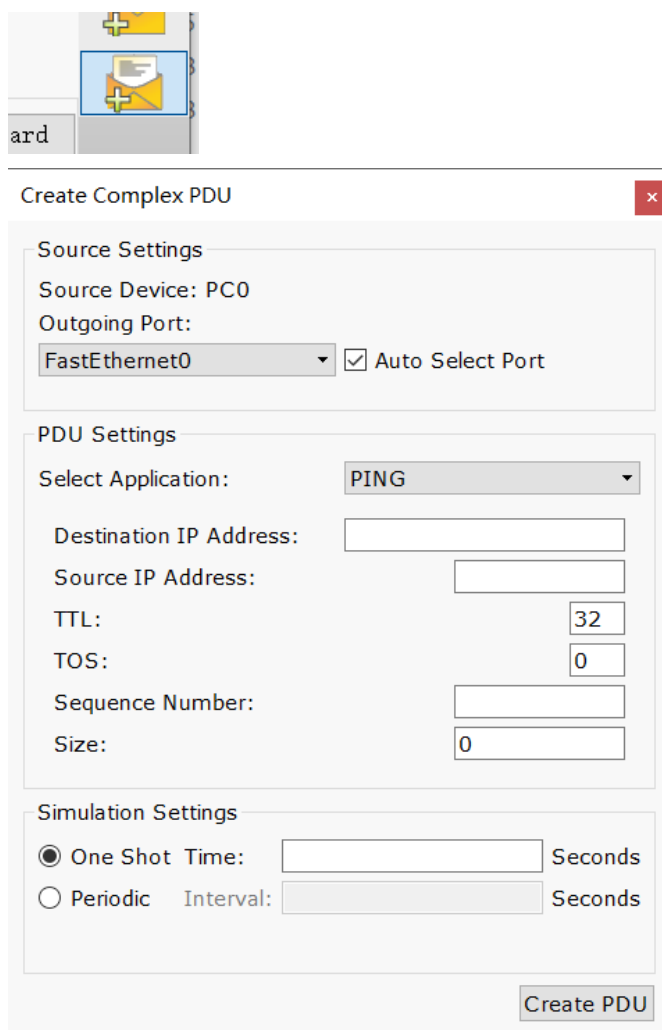
ICMP

0 8 16 31 Bits			
TYPE:	CODE:	CHECKSUM	
ID: 0x4	SEQ NUMBER: 6		

步骤 1 中，目的 IP 与主机不在同一网段，需要通过网关找到下一跳地址，而在该步骤中，如果地址设置为 192.168.253.1，直接在命令行输入 ping 指令，很明显会出现错误，因为中间路由器的接口 FastEthernet0/0、0/1 的 IP 地址还没变化，与当前主机设置的 IP 地址不匹配，因此会出现上述现象。

因为访问无法到达，因此参与的设备没有服务器，只有 PC 和路由器。

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。

Create Complex PDU

Source Settings

Source Device: PC0  
Outgoing Port:  
FastEthernet0
☒ Auto Select Port

PDU Settings

Select Application: PING  
Destination IP Address: 192.168.254.254  
Source IP Address:   
TTL: 1  
TOS: 0  
Sequence Number: 1  
Size: 0

Simulation Settings

☐ One Shot Time: Seconds  
☒ Periodic Interval: 2 Seconds

Create PDU

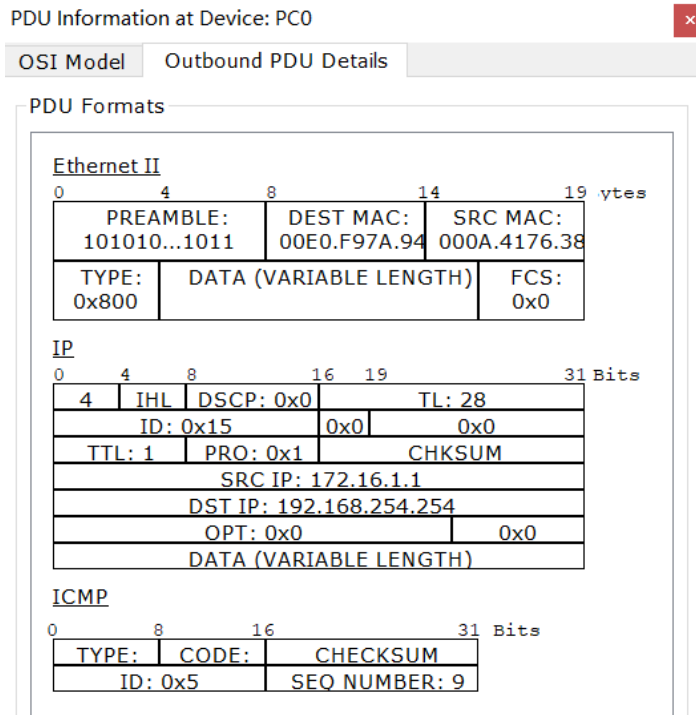
重复单击 Capture/Forward（捕获/转发）按钮，以在 Pod PC 与路由器之间生成多次交换。在 Event List（事件列表）中找到第一个数据包，即第一个回应请求。

Simulation Panel

Event List

Vis.	Time(s)	Last Dev	At Dev	Type	Info
	0.000	--	PC0	IC...	
	0.001	PC0	Router0	IC...	
	0.001	--	Router0	IC...	
	0.002	Router0	PC0	IC...	
	2.000	--	PC0	IC...	

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。



### 任务 3：检查 ARP 交换：

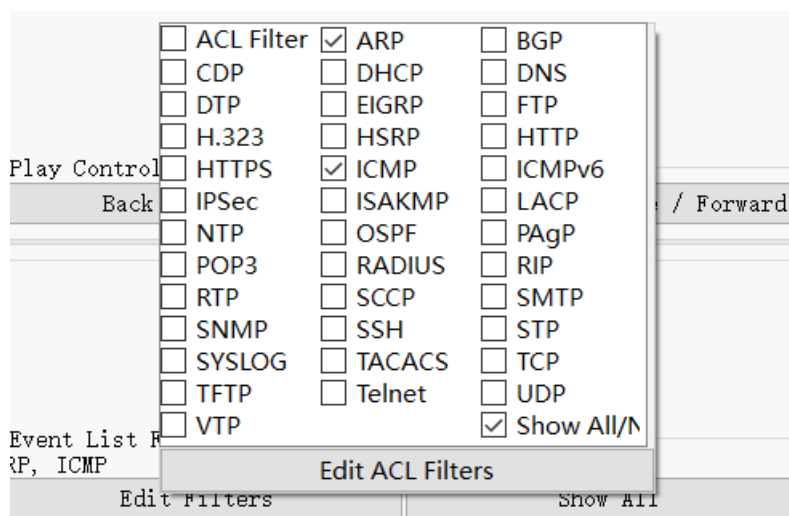
在 PC 1A 上使用 Packet Tracer 命令 arp -d。然后 Ping 地址 192.168.254.254。

```
PC>arp -d
PC>ping 192.168.254.254

Pinging 192.168.254.254 with 32 bytes of data:

Reply from 192.168.254.254: bytes=32 time=8ms TTL=127
```

packet tracer 中设置捕获 ARP 包：





	0.000	--	PC0	ARP	
	0.000	--	PC0	ICMP	
	0.000	--	PC0	ARP	
	0.001	--	PC0	ARP	
	0.001	PC0	Router0	ICMP	

查看 ARP 包:

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19 ytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FF	SRC MAC: 000A.4176.38	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

ARP

0	8	16	31 Bits
HARDWARE TYPE:		PROTOCOL TYPE:	
HLEN:	PLEN:	OPCODE: 0x1	
SOURCE MAC: 000A.4176.3881 (48		SOURCE IP (32 bits)	
172.16.1.1			
TARGET MAC: 0000.0000.0000 (48 bits			
TARGET IP: 172.16.1.1 (32 bits)			

PDU Information at Device: Router0

OSI Model

Inbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19 ytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FF	SRC MAC: 000A.4176.38	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0

ARP

0	8	16	31 Bits
HARDWARE TYPE:		PROTOCOL TYPE:	
HLEN:	PLEN:	OPCODE: 0x1	
SOURCE MAC: 000A.4176.3881 (48		SOURCE IP (32 bits)	
172.16.1.1			
TARGET MAC: 0000.0000.0000 (48 bits			
TARGET IP: 172.16.1.1 (32 bits)			

实验思考:

ARP 报文具体格式:

硬件类型		协议类型
硬件地址长度	协议长度	操作类型
发送方硬件地址 (0-3字节)		
发送方硬件地址 (4-5字节)		发送方IP地址 (0-1字节)
发送方IP地址 (2-3字节)		目标硬件地址 (0-1字节)
目标硬件地址 (2-5字节)		
目标IP地址 (0-3字节)		

各部分解释如下:

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): 源主机硬件地址的前 2 个字节;

发送方 IP 地址 (2-3 字节): 源主机硬件地址的后 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。