

计算机网络LAB4

姓名：姚丁钰

班级：智能2103班

学号：202107030125

实验目的

实验内容

路由器交换机的基本配置

路由器的一些基本配置

静态路由

子网划分

配置RIP

交换机的基本配置

了解ICMP数据包的格式

任务：使用Packet Tracer捕获和研究 ICMP 报文

检查ARP交换

任务 1：使用 Packet Tracer 的 arp 命令

任务 2：使用 Packet Tracer 检查 ARP 交换

实验总结

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

实验内容

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.路由器的一些基本配置.pkt ←


8.静态路由.pkt


15.子网划分.pkt


16.配置RIP.pkt


11.交换机的基本配置.pkt ←

路由器的一些基本配置



单击路由器0，在CIL中输入以下命令

```
1 R1>show version
2 此命令结果包含有IOS版本，IOS映像文件，
3 存储器大小，接口类型及配置登记值等信息。
4
5 Router>enable
6 Router#configure terminal
7 Router(config)#hostname R1
8
9 R1(config)#no ip domain-lookup
10 关闭域名解释
11
12 R1(config)#line console 0
13 R1(config-line)#logging synchronous
14 设置输入同步
15
16 R1(config-line)#exec-timeout 20 00
17 设置执行会话时间
18 R1(config-line)#end
```

```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T
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.

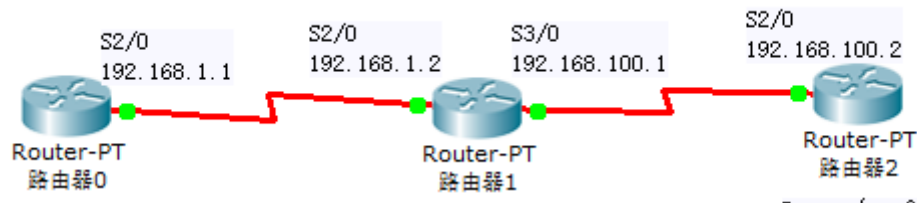
System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"
```

```

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 2000
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

静态路由



转发数据包是路由器的最主要功能。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。虽然静态路由不适合于在大的网络中使用，但是由于静态路由简单、路由器负载小、可控性强等原因，在许多场合中还经常被使用。

路由器在转发数据时，要先在路由表（routing table）中查找相应的路由。路由器有这么三种途径建立路由：

- (1) 直连网络：路由器自动添加和自己直接连接的网路的路由
- (2) 静态路由：管理员手动输入到路由器的路由
- (3) 动态路由：由路由协议（routing protocol）动态建立的路由

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**。

1. 对路由器0进行配置

```
1 Router(config)#hostname R1
2 R1(config)#int loopback0
3 R1(config-if)#ip address 1.1.1.1 255.255.255.0
4 R1(config-if)#exit
5 R1(config)#int s2/0
6 R1(config-if)#ip address 192.168.1.1 255.255.255.0
7 R1(config-if)#no shutdown
8 R1(config-if)#clock rate 64000
9 R1(config)#ip route 2.2.2.0 255.255.255.0 s2/0
10 下一跳为接口形式，s2/0是点对点的链路，注意应该是R1上的s2/0接口
11 R1(config)#ip route 3.3.3.0 255.255.255.0 192.168.1.2
12 下一跳为IP地址形式，192.168.1.2 是R2上的IP地址
13 R1#show ip route
```

```
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)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

2. 对路由器1进行配置

```
1 Router(config)#hostname R2
2 R2(config)#int loopback0
3 R2(config-if)#ip address 2.2.2.2 255.255.255.0
4 R2(config-if)#exit
5 R2(config)#int s2/0
6 R2(config-if)#ip address 192.168.1.2 255.255.255.0
7 R2(config-if)#no shutdown
8 R2(config-if)#exit
9 R2(config)#int s3/0
10 R2(config-if)#ip address 192.168.100.1 255.255.255.0
11 R2(config-if)#no shutdown
12 R2(config-if)#clock rate 64000
13 R2(config)#ip route 1.1.1.0 255.255.255.0 s2/0
14 R2(config)#ip route 3.3.3.0 255.255.255.0 s3/0
```

```

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int loopback0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#exit
R2(config)#int s2/0
R2(config-if)#ip add 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 add 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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

```

3. 对路由器2进行配置

```

1 Router(config)#hostname R3
2 R3(config)#int loopback0
3 R3(config-if)#ip address 3.3.3.3 255.255.255.0
4 R3(config-if)#exit
5 R3(config)#int s2/0
6 R3(config-if)#ip address 192.168.100.2 255.255.255.0
7 R3(config-if)#no shutdown
8 R3(config)#ip route 1.1.1.0 255.255.255.0 s2/0
9 R3(config)#ip route 2.2.2.0 255.255.255.0 s2/0
10 R3#show ip route

```

```

R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z
R3(config)#hostname R3
R3(config)#int loopback
% Incomplete command.
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)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

```

4. 在R1上执行ping命令进行测试

```

1
2 R1#ping

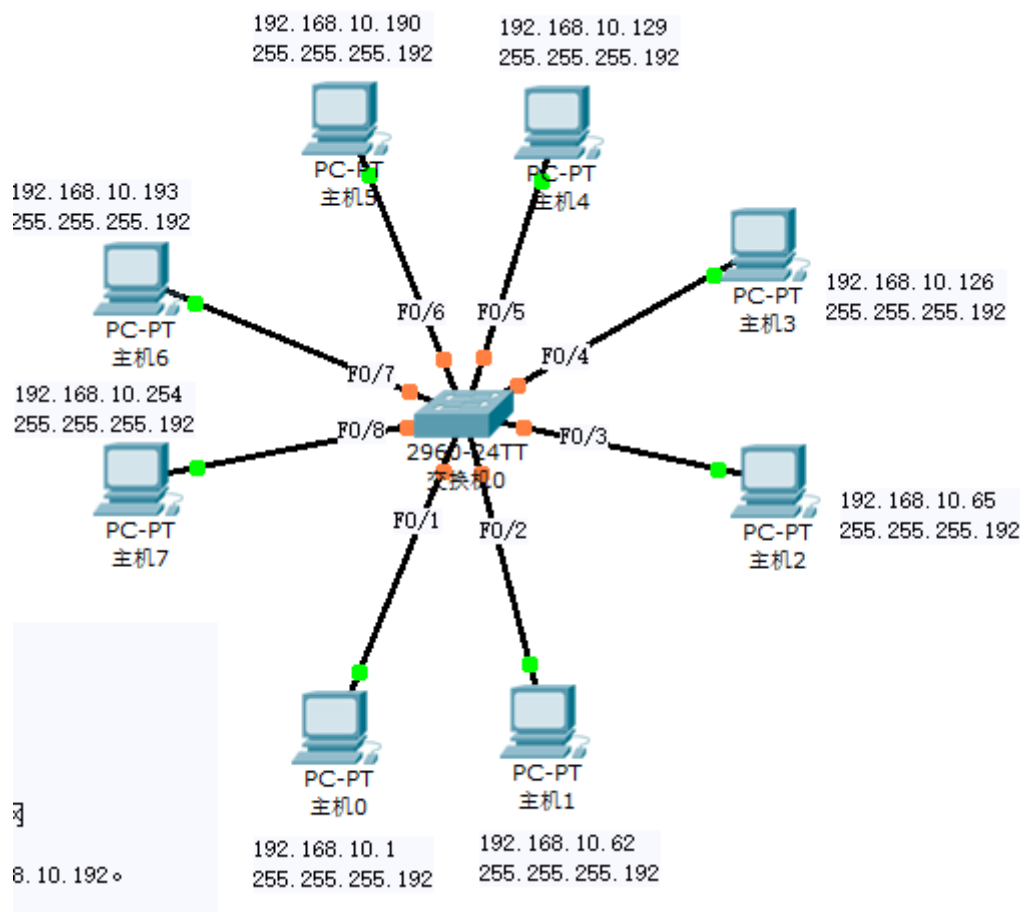
```

```
3 Protocol [ip]:
4 Target IP address: 2.2.2.2
5 Repeat count [5]:
6 Datagram size [100]:
7 Timeout in seconds [2]:
8 Extended commands [n]: y
9 Source address or interface: 1.1.1.1
10 Type of service [0]:
11 Set DF bit in IP header? [no]:
12 Validate reply data? [no]:
13 Data pattern [0xABCD]:
14 Loose, Strict, Record, Timestamp, Verbose[none]:
15 Sweep range of sizes [n]:
16 Type escape sequence to abort.
17 Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2
   seconds:
18 Packet sent with a source address of 1.1.1.1
19 !!!!!
```

```
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 = 20/28/31 ms
```

可以看到能够ping通2.2.2.2，因此配置信息无误

子网划分



1 划分子网的一些公式：

2

3 1.你所选择的子网掩码将会产生多少个子网：

4 2的x次方（x代表被借走的主机位数）。

5

6 2.每个子网有多少主机：2的y次方-2（y代

7 表被借走之后剩余的主机位数）。

8

9 3.有效子网是：有效子网号=256-十进制的子

10 网掩码（结果叫做block size）。

11

12 4.每个子网的广播地址是：广播地址=下个子

13 网号-1

14

15 5.每个子网的有效主机分别是：忽略子网内全

16 为0和全为1的地址剩下的就是有效主机地址。

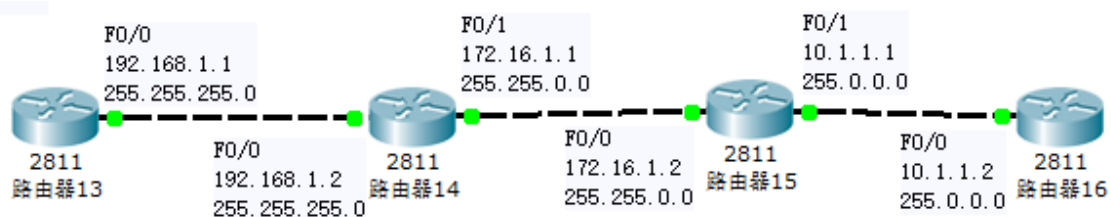
17 最后有效的1个主机地址=下个网号-2（即广

18 播地址-1）

1 网络地址192.168.10.0 子网掩码255.255.255.192

- 2
- 3 1.子网数=2的2次方=4。
- 4
- 5 2.每个子网的主机数=2的6次方-2=62。
- 6
- 7 3.有效子网: block size=256-192=64, 第一个子网
- 8 为192.168.10.0, 第二个子网为192.168.10.64,
- 9 第三个子网为192.168.10.128, 最后一个为192.168.10.192。
- 10
- 11 4.广播地址: 下个子网-1, 第一个子网的广播地址是192.168.10.63,
- 12 第二个是192.168.10.127, 第三个是192.168.10.191,
- 13 最后一个为192.168.10.255。
- 14
- 15 5.有效主机范围是: 第一个子网的主机地址是192.168.10.1到
- 16 192.168.10.62, 第二个是192.168.10.65到192.168.10.126,
- 17 第三个是192.168.10.129到192.168.10.190, 最后一个为
- 18 192.168.10.193到192.168.10.254。

配置RIP



- 1 路由选择信息协议 (RIP/RIP2/RIPng: Routing Information Protocol)
- 2
- 3 路由协议 默认管理距离
- 4
- 5 直连网络 0
- 6 静态路由 1
- 7 EIGRP(internal) 90
- 8 IGRP 100
- 9 OSPF 110
- 10 RIPv1/RIPv2 120
- 11
- 12 管理距离越小, 可信度越高, 优先采用可信度高的路由协议。

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——R4的配置信息如下:


```
1 R1#show ip protocols
2 R1(config)#router rip
3 R1(config-router)#network 192.168.1.0
4 R1(config-router)#end
5 R1#show ip route
6 R1#clear ip route *
7 R1#show ip route
```

```
1 R2(config)#router rip
2 R2(config-router)#network 192.168.1.0
3 R2(config-router)#network 172.16.0.0
4 R2(config-router)#end
5 R2#show ip route
6 R2#clear ip route *
7 R2#show ip route
```

```
1 R3(config)#router rip
2 R3(config-router)#network 172.16.0.0
3 R3(config-router)#network 10.0.0.0
4 R3(config-router)#end
5 R3#show ip route
```

```
1 R4(config)#router rip
2 R4(config-router)#network 10.0.0.0
3 R4(config-router)#end
4 R4#show ip protocols
5 R4#show ip route
```

```
R1>enable
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
```

```
R2>en
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
```

```

R3>en
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

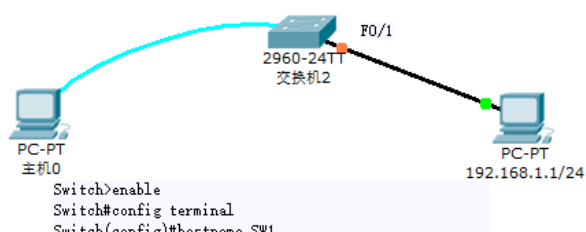
```

```

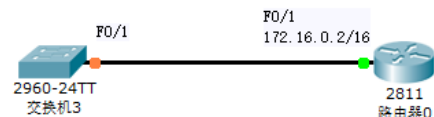
R4>en
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router rip
R4(config-router)#network 10.0.0.0
R4(config-router)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console

```

交换机的基本配置



交换机的商品安全：
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这里限制f0/1 接口只允许R1 接入。



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 (Context

Address 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

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，如图12-1：

(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，是介于前两者之间的一种解决方法。无碎片方法在读取数据帧

的长前64个字节后，就开始转发该帧。这种方式虽然也不提供数据校验，但是能够避免大多

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。

1. 交换机基本配置

```

1 Switch>en
2 Switch#conf t
3 Switch(config)#hostname S1
4 S1(config)#no ip domain-lookup
5 关闭域名查找
6 S1(config)#line console 0
7 S1(config-line)#logging synchronous
8 设置输入同步
9 S1(config-line)#exec-timeout 10 00
10 设置执行会话时间
11 S1(config-line)#end

```

```

S1>en
S1>enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 10 00
R1(config-line)#ennnd
      ^
% Invalid input detected at '^' marker.

R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

```

2. 交换机SW1配置

```

1 Switch>enable
2 Switch#config terminal
3 Switch(config)#hostname SW1
4 配置主机名
5 SW1(config)#enable secret cisco
6 配置密码
7 SW1(config)#line vty 0 15
8 SW1(config-line)#password cisco
9 SW1(config-line)#login
10
11 默认时交换机的以太网接口是开启的。对于交换机的
12 以太网口可以配置其双工模式、速率等。
13
14 SW1(config)#interface f0/1
15
16 SW1(config-if)#duplex auto
17 duplex 用来配置接口的双工模式，full—全双工、

```

```

18 half--半双工、auto--自动检测双工的模式
19
20 SW1(config-if)#speed auto
21 speed 命令用来配置交换机的接口速度，10--10M、
22 100--100M、1000--1000M、auto--自动检测接
23 口速度。
24
25 SW1(config)#int vlan 1
26 SW1(config-if)#ip add 192.168.1.254 255.255.255.0
27 SW1(config-if)#no shutdown
28 SW1(config)#ip default-gateway 192.168.1.100
29 交换机也允许被telnet，这时需要在交换机上配置一个IP
30 地址，这个地址是在VLAN 接口上配置的
31 以上在VLAN 1 接口上配置了管理地址，接在VLAN 1上的
32 计算机可以直接进行telnet该地址。为了其他网段的计算
33 机也可以telnet 交换机，我们在交换机上配置了缺省网关。
34
35 SW1#copy running-config startup-config
36 保存配置

```

```

SW1>en
Password:
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#hostname SW1
SW1(config)#enable secret cisco
SW1(config)#line vty 0 15
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#interface f0/1
SW1(config-if)#duplex auto
SW1(config-if)#speed auto
SW1(config-if)#int vlan
^
% Invalid input detected at '^' marker.

SW1(config-if)#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

```

3. SW1的安全配置

```

1 SW1(config)#int f0/1
2 SW1(config-if)#switch mode access
3 以上命令把端口改为访问模式，即用来接入计算机
4
5 SW1(config-if)#switch port-security
6 打开交换机的端口安全功能。

```

```

7
8 SW1(config-if)#switch port-security maximum 1
9 只允许该端口下的MAC 条目最大数量为1，即只允许一个设备接入
10
11 SW1(config-if)#switch port-security violation shutdown
12 S1(config-if)#switch port-security violation { protect |
  shutdown | restrict }
13
14     protect:当新的计算机接入时，如果该接口的MAC 条目超过最大数
15 量，则这个新的计算
16 机将无法接入，而原有的计算机不受影响
17
18     ?? shutdown:当新的计算机接入时，如果该接口的MAC 条目超过最大数
19 量，则该接口将会
20 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
21 “no shutdown”
22 命令重新打开。
23
24     ?? restrict:当新的计算机接入时，如果该接口的MAC 条目超过最大数
25 量，则这个新的计
26 算机可以接入，然而交换机将向发送警告信息。
27
28 SW1(config-if)#switchport port-security mac-address
29 0001.63e1.9702
30 允许R1路由器从F0/1接口接入
31
32 SW1(config-if)#shutdown
33 SW1(config-if)#no shutdown
34
35 SW1(config)#int vlan 1
36 SW1(config-if)#no shut
37 SW1(config-if)#ip add 172.16.0.1 255.255.0.0
38 配置交换机的管理地址
39
40 SW1#show mac-address-table
41
42     Mac Address Table
43
44     -----
45
46     Vlan      Mac Address      Type      Ports
47     ----      -
48
49     1         0001.63e1.9702   STATIC    Fa0/1
50
51 R1的MAC已经被登记在f0/1接口，并且表明是静态加入的
52

```

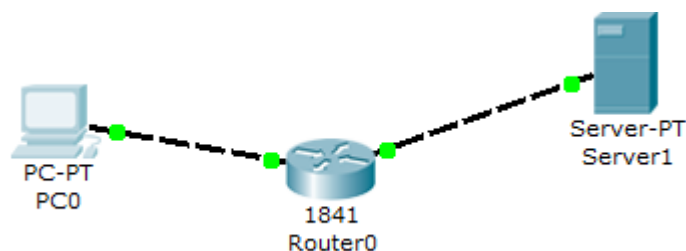
```
43 SW1#show int f0/1
44 FastEthernet0/1 is down, line protocol is down (err-
disabled)
45   Hardware is Lance, address is 00e0.f714.de01 (bia
00e0.f714.de01)
46   MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
47   reliability 255/255, txload 1/255, rxload 1/255
48 以上表明F0/1接口因为错误而被关闭。非法设备移除后，在F0/1接口下，
  执行“shutdown”
49 和“no shutdown”命令可以重新打开该接口。
50
51 SW1#show port-security
52 可以查看端口安全的设置情况
```

```
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 violation shutdown
```

了解ICMP数据包的格式

任务：使用Packet Tracer捕获和研究 ICMP 报文

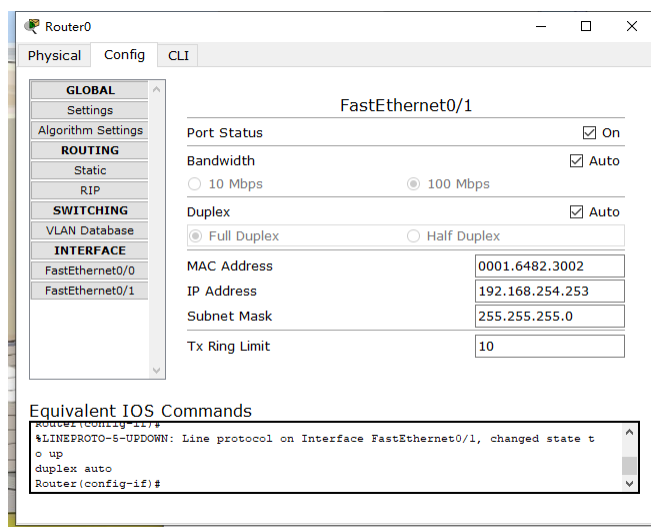
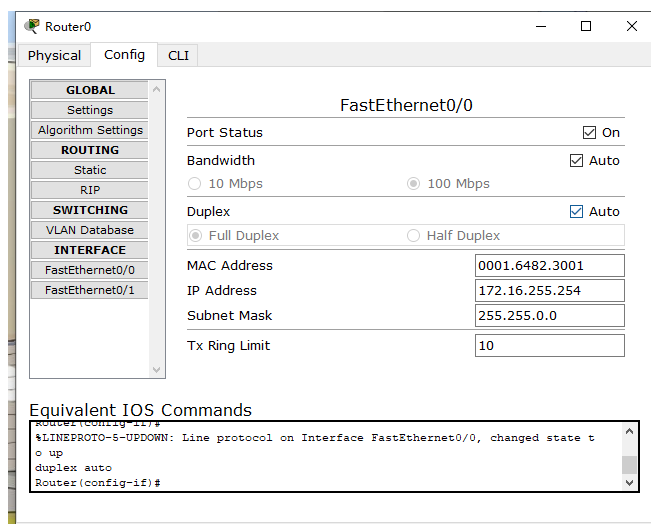
实验拓扑图：



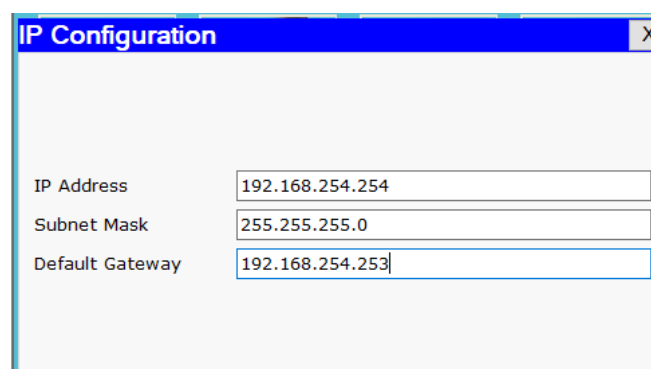
1. PC0的IP配置

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IP Address	176.16.1.1
Subnet Mask	255.255.0.0
Default Gateway	176.16.255.254
DNS Server	176.16.255.254

2. 路由器配置



3. 服务器配置



捕获 ICMP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）。


```




















PC>ping 192.168.254.254

Pinging 192.168.254.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.254.254: bytes=32 time=4ms TTL=127
Reply from 192.168.254.254: bytes=32 time=4ms TTL=127
Reply from 192.168.254.254: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

```

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.003	--	PC0	ICMP	
	0.004	PC0	Router0	ICMP	
	6.007	--	PC0	ICMP	
	6.008	PC0	Router0	ICMP	
	6.009	Router0	Server0	ICMP	
	6.010	Server0	Router0	ICMP	
	6.011	Router0	PC0	ICMP	
	7.014	--	PC0	ICMP	
	7.015	PC0	Router0	ICMP	
	7.016	Router0	Server0	ICMP	
	7.017	Server0	Router0	ICMP	
	7.018	Router0	PC0	ICMP	
	8.018	--	PC0	ICMP	
	8.019	PC0	Router0	ICMP	
	8.020	Router0	Server0	ICMP	
	8.021	Server0	Router0	ICMP	
	8.022	Router0	PC0	ICMP	

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

At Device: PC0
Source: PC0
Destination: 192.168.254.254

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 172.16.1.1, Dest. IP: 192.168.254.254 ICMP Message Type: 8
Layer2	Layer 2: Ethernet II Header 000B.BE78.6A19 >> 0060.7049.AD01
Layer1	Layer 1: Port(s): FastEthernet

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

Challenge Me << Previous Layer Next Layer >>

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: 0060.7049.AD01				SRC MAC: 000B.BE78.6A19			
TYPE: 0x800		DATA (VARIABLE LENGTH)						FCS: 0x0			

IP

0		4		8		16		19		31		Bits	
4		IHL		DSCP: 0x0		TL: 128							
ID: 0x26				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: 0x8		CODE: 0x0		CHECKSUM					
ID: 0x7				SEQ NUMBER: 22					

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。

请求报文(类型为 8)和应答报文(类型为 0)。

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

Ping statistics for 192.168.253.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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: FastEthernet ☒ 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。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。

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.001	PC0	Router0	ICMP	
	0.001	--	Router0	ICMP	
	0.002	Router0	PC0	ICMP	
	2.000	--	PC0	ICMP	
	2.001	PC0	Router0	ICMP	
	2.001	--	Router0	ICMP	
	2.002	Router0	PC0	ICMP	
	4.000	--	PC0	ICMP	
	4.001	PC0	Router0	ICMP	
	4.001	--	Router0	ICMP	
	4.002	Router0	PC0	ICMP	
	6.000	--	PC0	ICMP	

PDU Information at Device: PC0

OSI Model Outbound PDU Details

At Device: PC0
Source: PC0
Destination: 192.168.254.254

In Layers
Layer7
Layer6
Layer5
Layer4

Layer3

Layer2
Layer1

Out Layers
Layer7
Layer6
Layer5
Layer4

Layer 3: IP Header Src. IP: 172.16.1.1, Dest. IP: 192.168.254.254 ICMP Message Type: 8

Layer 2: Ethernet II Header 000B.BE78.6A19 >> 0060.7049.AD01

Layer 1: Port(s): FastEthernet

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The device sets TTL in the packet header.
5. The destination IP address is not in the same subnet and is not the broadcast address.
6. The default gateway is set. The device sets the next-hop to default gateway.

Challenge Me << Previous Layer Next Layer >>

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: 0060.7049.AD01				SRC MAC: 000B.BE78.6A19			
TYPE: 0x800		DATA (VARIABLE LENGTH)						FCS: 0x0			

IP

0		4		8		16		19		31		Bits
4		IHL		DSCP: 0x0		TL: 28						
ID: 0x3b				0x0		0x0						
TTL: 1		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: 0x8		CODE: 0x0		CHECKSUM				
ID: 0x14		SEQ NUMBER: 43						

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。

ARP协议工作过程

主机A的IP地址为192.168.1.1，MAC地址为0A-11-22-33-44-01；

主机B的IP地址为192.168.1.2，MAC地址为0A-11-22-33-44-02；

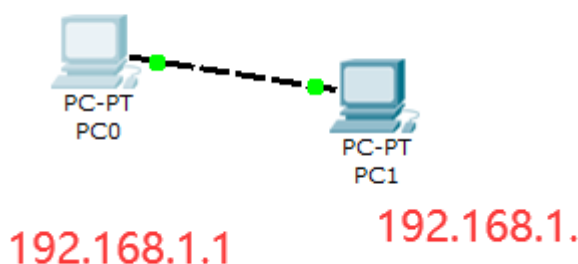
当主机A要与主机B通信时，地址解析协议可以将主机B的IP地址（192.168.1.2）解析成主机B的MAC地址，以下为工作流程：

1. 根据主机A上的路由表内容，IP确定用于访问主机B的转发IP地址是192.168.1.2。然后A主机在自己的本地ARP缓存中检查主机B的匹配MAC地址。
2. 如果主机A在ARP缓存中没有找到映射，它将询问192.168.1.2的硬件地址，从而将ARP请求帧广播到本地网络上的所有主机。源主机A的IP地址和MAC地址都包括在ARP请求中。本地网络上的每台主机都接收到ARP请求并且检查是否与自己的IP地址匹配。如果主机发现请求的IP地址与自己的IP地址不匹配，它将丢弃ARP请求。
3. 主机B确定ARP请求中的IP地址与自己的IP地址匹配，则将主机A的IP地址和MAC地址映射添加到本地ARP缓存中。
4. 主机B将包含其MAC地址的ARP回复消息直接发送回主机A。
5. 当主机A收到从主机B发来的ARP回复消息时，会用主机B的IP和MAC地址映射更新ARP缓存。本机缓存是有生存期的，生存期结束后，将再次重复上面的过程。主机B的MAC地址一旦确定，主机A就能向主机B发送IP通信了。

ARP缓存

ARP缓存是个用来储存IP地址和MAC地址的缓冲区，其本质就是一个IP地址->MAC地址的对应表，表中每一个条目分别记录了网络上其他主机的IP地址和对应的MAC地址。每一个以太网或令牌环网络适配器都有自己单独的表。当地址解析协议被询问一个已知IP地址节点的MAC地址时，先在ARP缓存中查看，若存在，就直接返回与之对应的MAC地址，若不存在，才发送ARP请求向局域网查询。

建立拓扑图如下：



设置两个PC的IP地址分别如下：

- 192.168.1.1
- 192.168.1.2

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。

```
PC>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d
PC>
```

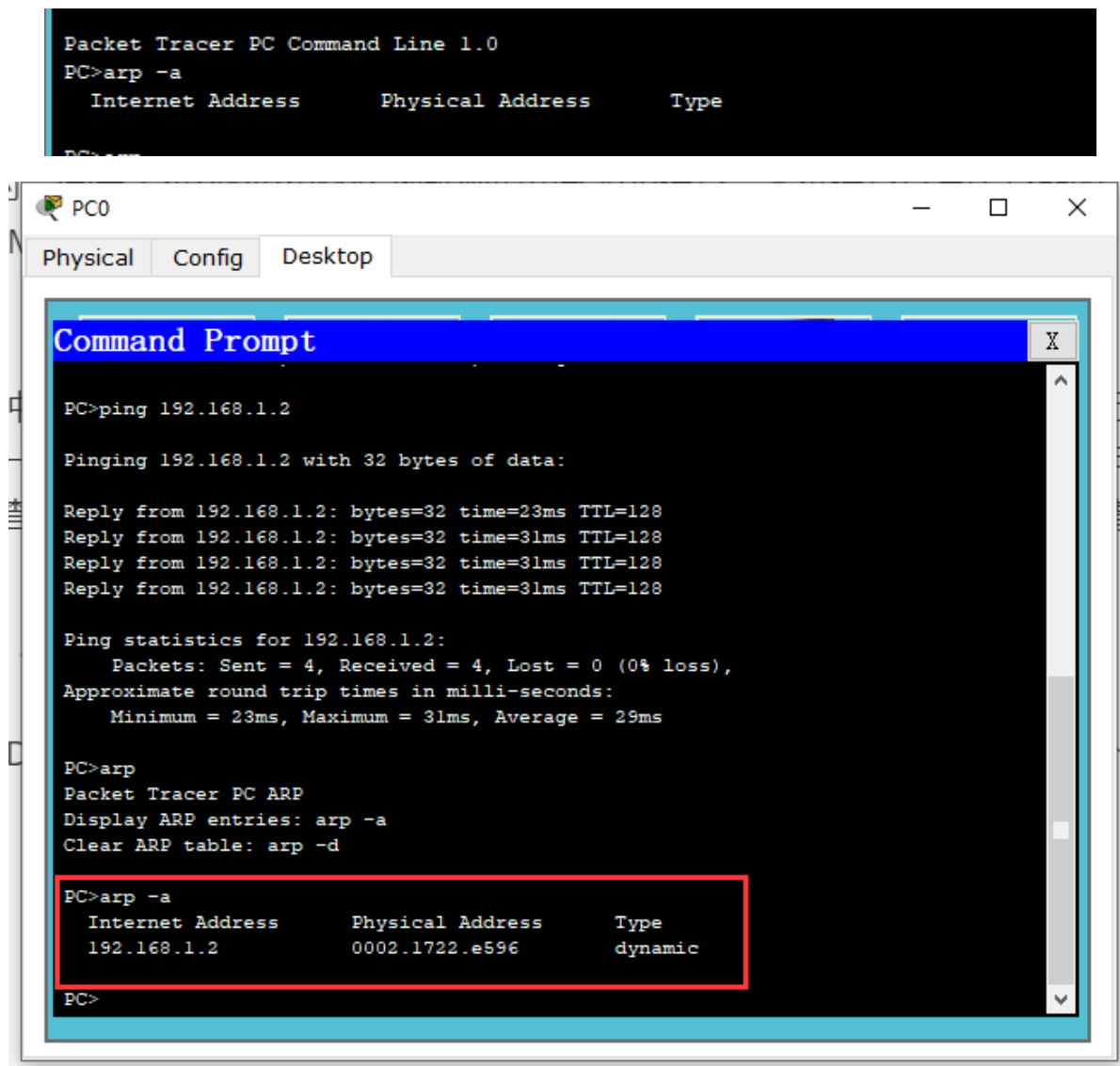
步骤 2. 使用 ping 命令在 ARP 缓存中动态添加条目。

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%。

【注意】这里没有用255.255.255.255，而是直接使用了目的ip地址，原因在于我们这里改变了拓扑图，使用了两个PC。如果是服务器的话可能会获得回应，但PC的操作系统不会回应广播的ping，只会响应明确地址且目标为自己的ping（这也是为了安全），所以我们这里直接ping对方，但不影响实验的效果。

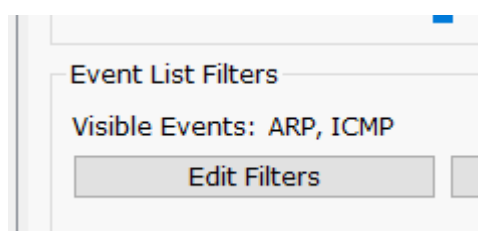


原来ARP表中是没有的，ping结束后有目标地址的表项。

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。

```
PC>arp -d
PC>arp -a
    Internet Address      Physical Address      Type
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=5ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms

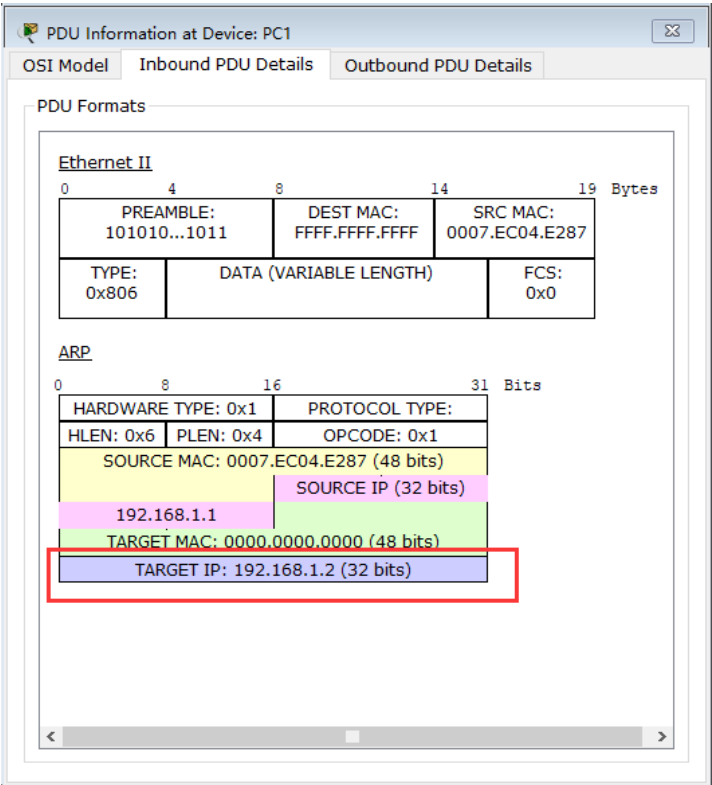
PC>arp -a
    Internet Address      Physical Address      Type
192.168.1.2              0002.1722.e596       dynamic
```

步骤 3. 捕获并评估 ARP 通信。

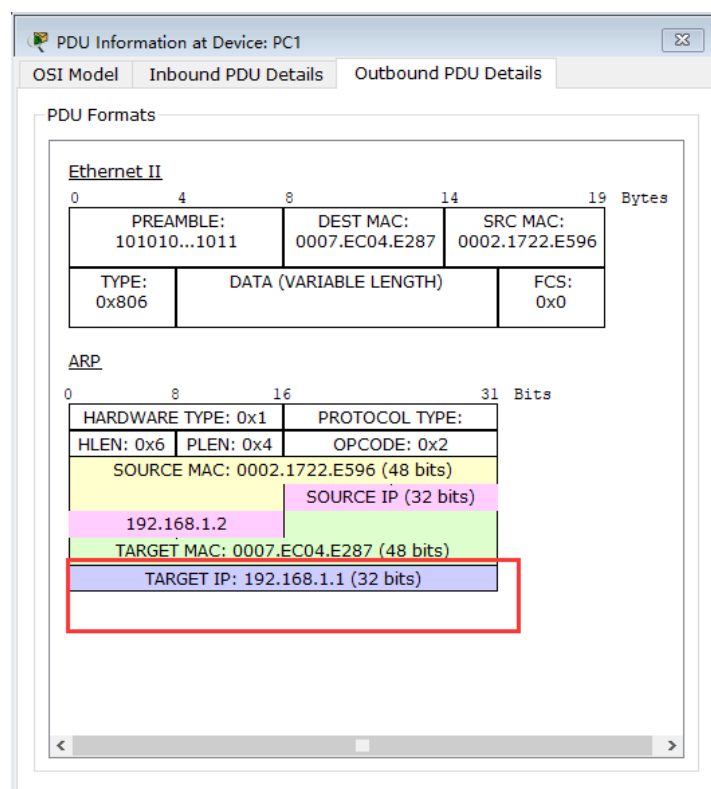
在发出 ping 命令之后，单击 Auto Capture/Play（自动捕获/播放）捕获数据包。当 Buffer Full（缓冲区已满）窗口打开时，单击 View Previous Events（查看以前的事件）按钮。

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ARP	
	0.000	--	PC0	ICMP	
	0.000	--	PC0	ARP	
	0.001	PC0	PC1	ARP	
	0.001	--	PC0	ARP	
	0.002	PC0	PC1	ARP	
	0.003	PC1	PC0	ARP	
	0.003	--	PC0	ICMP	
	0.004	PC0	PC1	ICMP	
	0.005	PC1	PC0	ICMP	
	1.008	--	PC0	ICMP	
	1.009	PC0	PC1	ICMP	
	1.010	PC1	PC0	ICMP	
	2.011	--	PC0	ICMP	
	2.012	PC0	PC1	ICMP	
	2.013	PC1	PC0	ICMP	
	3.014	--	PC0	ICMP	
	3.015	PC0	PC1	ICMP	

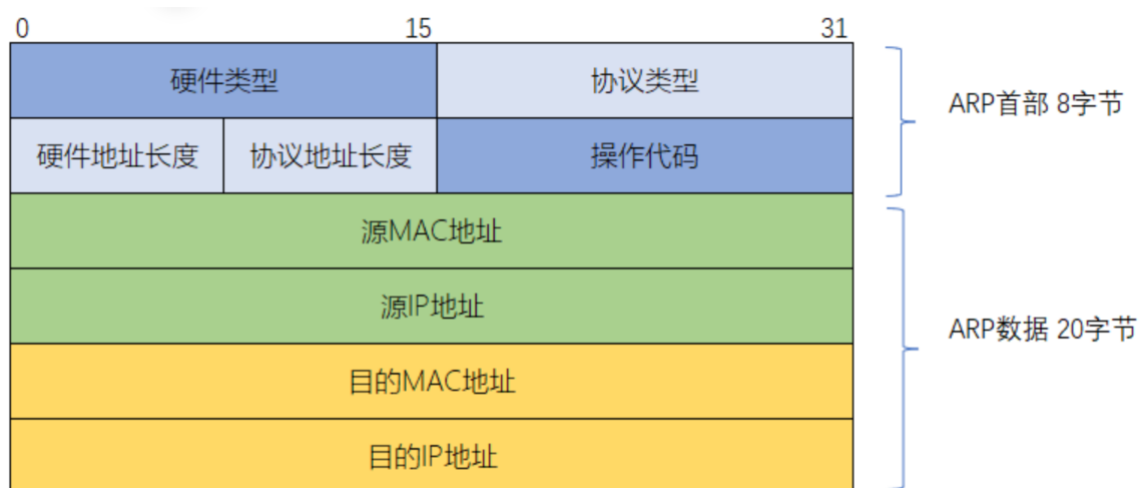
请求报文：任何时候，当主机需要找出这个网络中的另一个主机的物理地址时，它就可以发送一个ARP请求报文，这个报文包好了发送方的MAC地址和IP地址以及接收方的IP地址。因为发送方不知道接收方的物理地址，所以这个查询分组会在网络层中进行广播。



响应报文：局域网中的每一台主机都会接受并处理这个ARP请求报文，然后进行验证，查看接收方的IP地址是不是自己的地址，只有验证成功的主机才会返回一个ARP响应报文，这个响应报文包含接收方的IP地址和物理地址。这个报文利用收到的ARP请求报文中的请求方物理地址以单播的方式直接发送给ARP请求报文的请求方。



ARP报文格式如下：



CSDN @甘9

实验总结

通过PacketTracer工具对应用层和传输层协议进行分析，学会简单的使用该工具分析web请求、HTTP请求和FTP请求，对于应用层和传输层的几个协议理解更加深刻。

PacketTracer工具的应用在上学期的路由与交换技术课程中已经比较熟悉了，因此做这次实验比较顺利，这次模拟分析了web请求、HTTP请求、FTP请求，非常清楚地可以看到数据包在路径上的转移过程，非常形象的完成了对这三者的实际理解。

