实验 1：基本网络工具集使用和协议数据单元观测

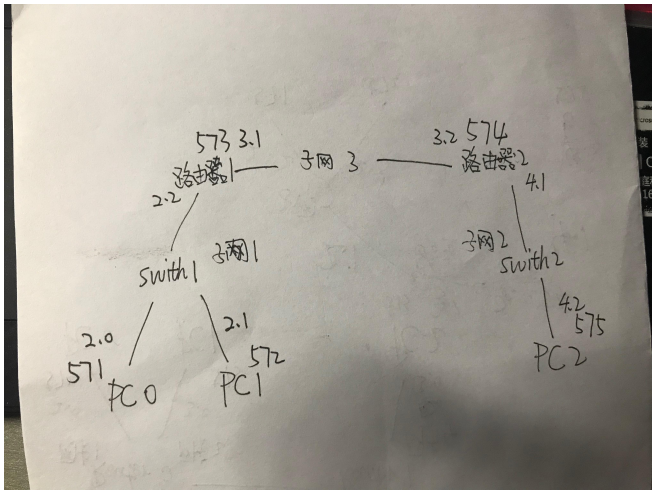
李杨 161220071

实验 1：

1. 利用 VMWare 搭建一个由 5 台虚拟机组成的随机拓扑网络。

实验目的：模拟并搭建拓扑网络，使得主机与路由器之间可以相互通信。

网络拓扑配置：



附表 1:

节点名	虚拟设备名	ip	netmask
Router0	573	192.168.2.2	255.255.255.0
		192.168.3.1	255.255.255.0
Router1	574	192.168.3.2	255.255.255.0
		192.168.4.1	255.255.255.0
Pc0	571	192.168.2.0	255.255.255.0

Pc1	572	192.168.2.1	255.255.255.0
Pc2	575	192.168.4.2	255.255.255.0

路由规则配置：

对于路由器 1 来说，有三条指令要配置，也就是它将三个子网串联起来的三条指令

Ip route add 192.168.2.0/24 via 192.168.2.2 将数据包通过 2.2 发送到子网 2

Ip route add 192.168.3.0/24 via 192.168.3.1 将数据包通过 3.1 发送到子网 3

Ip route add 192.168.4.0/24 via 192.168.3.2 将数据从子网 3 发送到子网 4

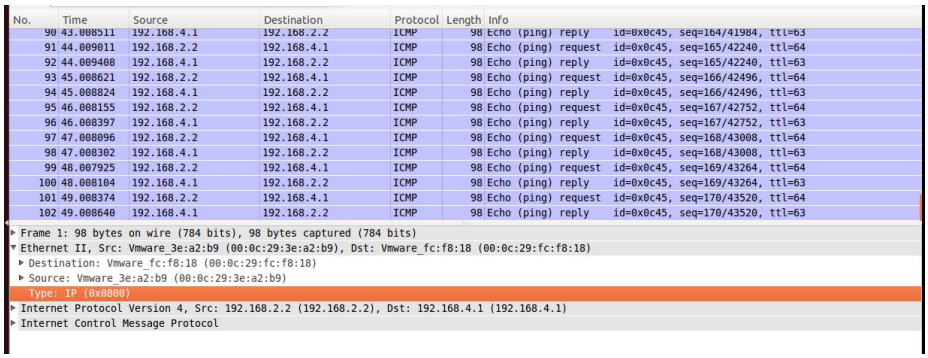
同理，路由器也有三条指令，分别是：

Ip route add 192.168.4.0/24 via 192.168.4.1

Ip route add 192.168.3.0/24 via 192.168.3.2

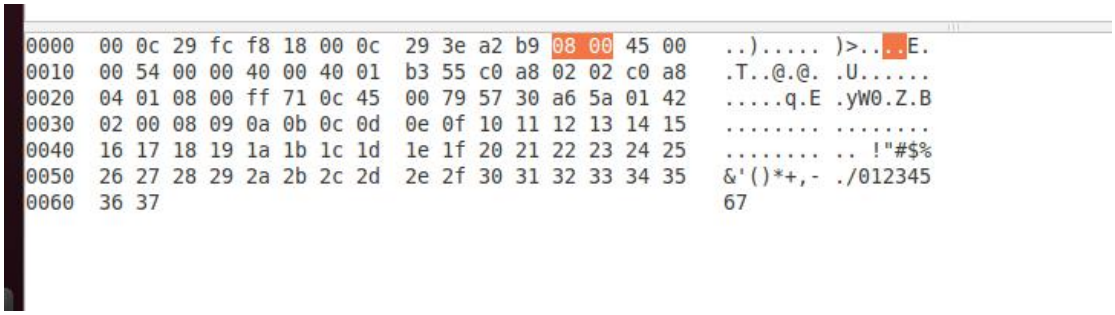
Ip route add 192.168.2.0/24 via 192.168.3.1

数据包截图：



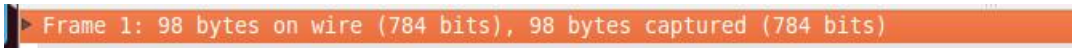
、

协议报文分析：



这是在 192.168.2.2 的地址上 ping 192.168.4.1

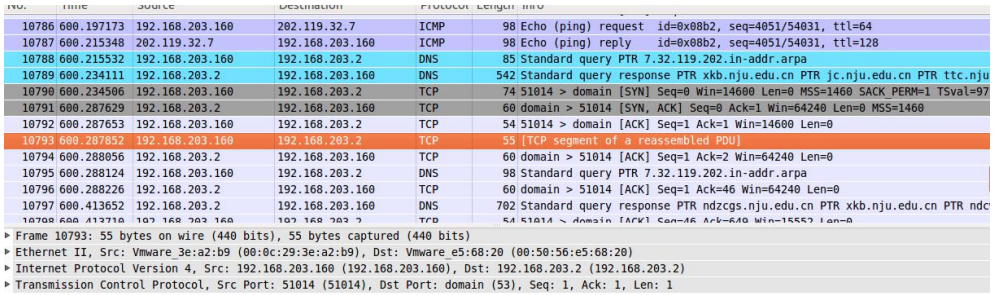
对应的是 c0 a8 02 02 c0 a8 04 01



这里应该是说明了捕获率为 100%，即丢包率为 0.、

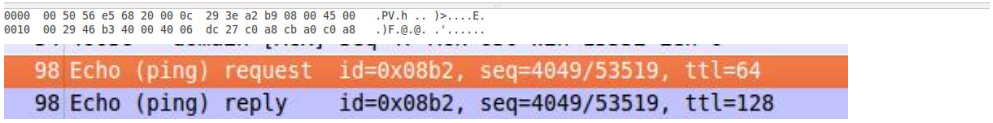
2：利用 wireshark 观测 PDU (ping 系主页）

PING cs.nju.edu.cn:



No.	Time	Source	Destination	Protocol	Length	Info
10786	600.197173	192.168.203.160	202.119.32.7	ICMP	98	Echo (ping) request id=0x08b2, seq=4051/54031, ttl=64
10787	600.215348	202.119.32.7	192.168.203.160	ICMP	98	Echo (ping) reply id=0x08b2, seq=4051/54031, ttl=128
10788	600.215532	192.168.203.160	192.168.203.2	DNS	85	Standard query PTR 7.32.119.202.in-addr.arpa
10789	600.234111	192.168.203.2	192.168.203.160	DNS	542	Standard query response PTR xkb.nju.edu.cn PTR jc.nju.edu.cn PTR ttc.nju
10790	600.234506	192.168.203.160	192.168.203.2	TCP	74	51014 > domain [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=97
10791	600.287629	192.168.203.2	192.168.203.160	TCP	60	domain > 51014 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10792	600.287653	192.168.203.160	192.168.203.2	TCP	54	51014 > domain [ACK] Seq=1 Ack=1 Win=14600 Len=0
10793	600.287852	192.168.203.160	192.168.203.2	TCP	55	[TCP segment of a reassembled PDU]
10794	600.288056	192.168.203.2	192.168.203.160	TCP	60	domain > 51014 [ACK] Seq=1 Ack=2 Win=64240 Len=0
10795	600.288124	192.168.203.160	192.168.203.2	DNS	98	Standard query PTR 7.32.119.202.in-addr.arpa
10796	600.288226	192.168.203.2	192.168.203.160	TCP	60	domain > 51014 [ACK] Seq=1 Ack=46 Win=64240 Len=0
10797	600.413652	192.168.203.2	192.168.203.160	DNS	702	Standard query response PTR ndzcgs.nju.edu.cn PTR xkb.nju.edu.cn PTR ndc

▸ Frame 10793: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
▸ Ethernet II, Src: Vmware_3e:a2:b9 (00:0c:29:3e:a2:b9), Dst: Vmware_e5:68:20 (00:50:56:e5:68:20)
▸ Internet Protocol Version 4, Src: 192.168.203.160 (192.168.203.160), Dst: 192.168.203.2 (192.168.203.2)
▸ Transmission Control Protocol, Src Port: 51014 (51014), Dst Port: domain (53), Seq: 1, Ack: 1, Len: 1



```
0000  00 50 56 e5 68 20 00 0c  29 3e a2 b9 08 00 45 00   .PV.h .. )>....E.
0010  00 29 46 b3 40 00 40 06  dc 27 c0 a8 cb a0 c0 a8   .)F.@.@. .'......
```

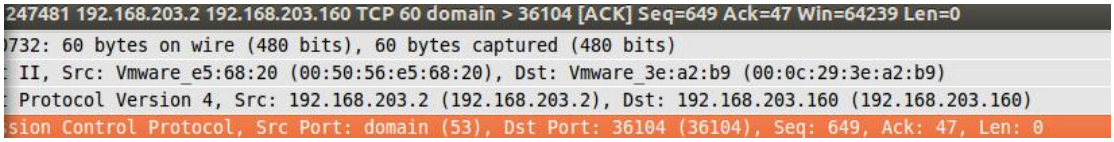
```
  98 Echo (ping) request  id=0x08b2, seq=4049/53519, ttl=64
  98 Echo (ping) reply    id=0x08b2, seq=4049/53519, ttl=128
```

第一个为 ping 请求指令，第二个为回应指令

98 表示 98byte 在传输

源计算机地址：192.168.203.2

目的计算机地址：192.168.203.160



```
247481 192.168.203.2 192.168.203.160 TCP 60 domain > 36104 [ACK] Seq=649 Ack=47 Win=64239 Len=0
732: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 II, Src: Vmware_e5:68:20 (00:50:56:e5:68:20), Dst: Vmware_3e:a2:b9 (00:0c:29:3e:a2:b9)
 Protocol Version 4, Src: 192.168.203.2 (192.168.203.2), Dst: 192.168.203.160 (192.168.203.160)
sion Control Protocol, Src Port: domain (53), Dst Port: 36104 (36104), Seq: 649, Ack: 47, Len: 0
```

ACK：是确认字符，在数据通信中，接收站发给发送站的一种传输类控制字符。表示发来的数据已确认接收无误。

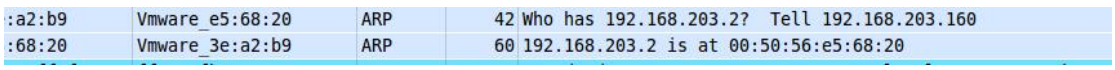
www.nju.edu.cn:

1	0.000000	111.13.101.73	192.168.203.160	TCP	60	http > 38421 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
2	0.000122	192.168.203.160	111.13.101.73	TCP	54	38421 > http [FIN, ACK] Seq=1 Ack=2 Win=15544 Len=0
3	0.000399	111.13.101.73	192.168.203.160	TCP	60	http > 38421 [ACK] Seq=2 Ack=2 Win=64239 Len=0
4	0.013365	111.13.100.35	192.168.203.160	TCP	60	http > 57652 [FIN, PSH, ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.013474	192.168.203.160	111.13.100.35	TCP	54	57652 > http [FIN, ACK] Seq=1 Ack=2 Win=15544 Len=0
6	0.013667	111.13.100.35	192.168.203.160	TCP	60	http > 57652 [ACK] Seq=2 Ack=2 Win=64239 Len=0
7	28.524745	192.168.203.160	192.168.203.2	DNS	82	Standard query A videosearch.ubuntu.com
8	28.538262	192.168.203.2	192.168.203.160	DNS	143	Standard query response, No such name
9	28.538437	192.168.203.160	192.168.203.2	DNS	94	Standard query A videosearch.ubuntu.com.localdomain
10	28.551507	192.168.203.2	192.168.203.160	DNS	94	Standard query response, No such name
11	86.149328	192.168.203.160	117.18.237.29	TCP	54	35923 > http [FIN, ACK] Seq=1 Ack=1 Win=15760 Len=0
12	86.149748	192.168.203.160	23.37.139.27	TCP	54	51290 > http [FIN, ACK] Seq=1 Ack=1 Win=15780 Len=0
13	86.150269	117.18.237.29	192.168.203.160	TCP	60	http > 35923 [ACK] Seq=1 Ack=2 Win=64239 Len=0

源计算机地址：192.168.203.2

目的计算机地址：192.168.203.160

中间经过了：111.13.101.73



```
:a2:b9  Vmware_e5:68:20  ARP  42  Who has 192.168.203.2?  Tell 192.168.203.160
:68:20  Vmware_3e:a2:b9  ARP  60  192.168.203.2 is at 00:50:56:e5:68:20
```

这里应该是向 192.168.203.160 说明要发送的信息所在的地址为 192.168.203.2　即 00:50:56：e5:68:20