

实验一 基本网络工具集使用和协议 数据单元（PDU）观测

邱梓豪

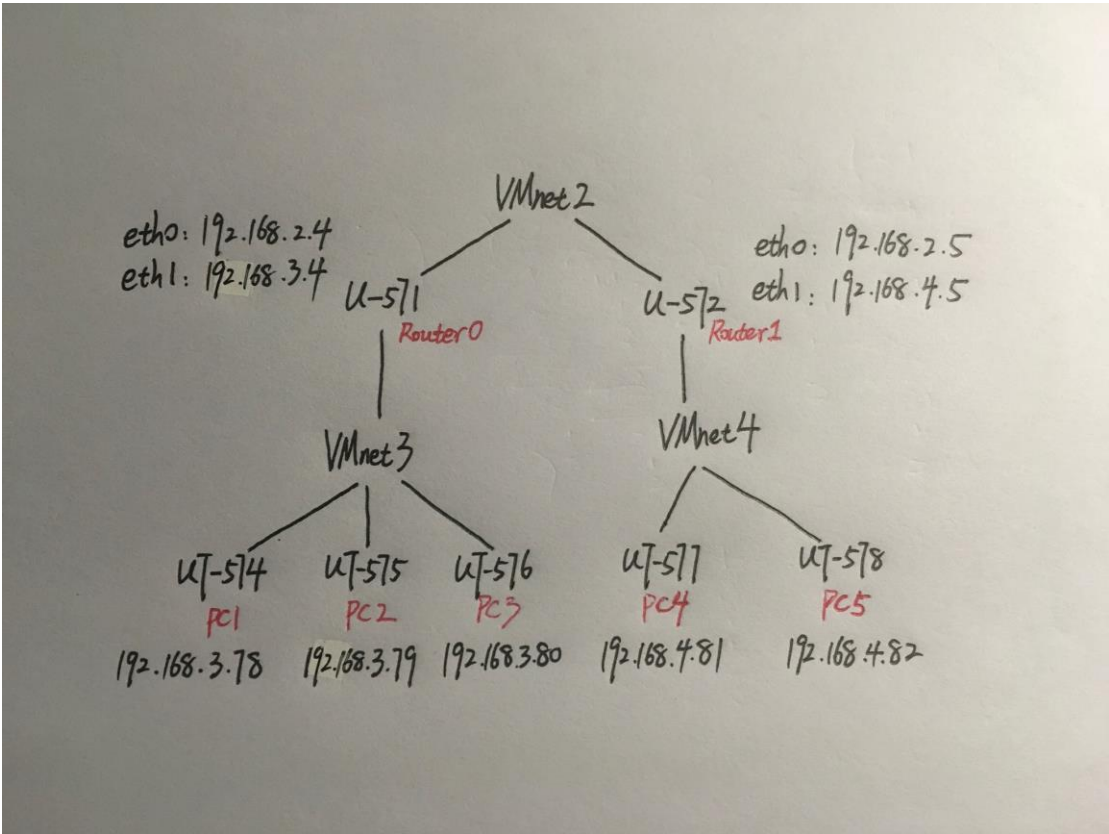
141130077

一、实验目的

本实验的主要目的是让学生了解在一个常见的 linux 系统中，熟悉系统最基本的网络工具集合（如 `ifconfig`，`route`，`wireshark` 等）的使用，并能够熟练观察和初步分析协议 PDU 的内容，为进一步的实验打下基础。

二、网络拓扑配置

网络拓扑结构：



相关结点的 ip 及 netmask 设置：

节点名	虚拟设备名	Ip	Netmask
Router0	U-571	Eth0: 192.168.2.4	255.255.255.0

		Eth1: 192.168.3.4	255.255.255.0
Router1	U-572	Eth0: 192.168.2.5	255.255.255.0
		Eth1: 192.168.4.5	255.255.255.0
PC1	UT-574	192.168.3.78	255.255.255.0
PC2	UT-575	192.168.3.79	255.255.255.0
PC3	UT-576	192.168.3.80	255.255.255.0
PC4	UT-577	192.168.4.81	255.255.255.0
PC5	UT-578	192.168.4.82	255.255.255.0

注意在虚拟机配置中确认每个 router 和 pc 的网络适配器!!

三、路由规则设置

Ip 设置命令:

```
Router0 U-571: sudo ifconfig eth0 192.168.2.4 netmask 255.255.255.0
               sudo ifconfig eth1 192.168.3.4 netmask 255.255.255.0
Router1 U-572: sudo ifconfig eth0 192.168.2.5 netmask 255.255.255.0
               sudo ifconfig eth1 192.168.4.5 netmask 255.255.255.0
PC1 UT-574:   sudo ifconfig eth0 192.168.3.78 netmask 255.255.255.0
PC2 UT-575:   sudo ifconfig eth0 192.168.3.79 netmask 255.255.255.0
PC3 UT-576:   sudo ifconfig eth0 192.168.3.80 netmask 255.255.255.0
PC4 UT-577:   sudo ifconfig eth0 192.168.4.81 netmask 255.255.255.0
PC5 UT-578:   sudo ifconfig eth0 192.168.4.82 netmask 255.255.255.0
```

网关设置命令:

```
Router0 U-571: sudo route add default gw 192.168.2.5
Router1 U-572: sudo route add default gw 192.168.2.4
PC1 UT-574:   sudo route add default gw 192.168.3.4
PC2 UT-575:   sudo route add default gw 192.168.3.4
PC3 UT-576:   sudo route add default gw 192.168.3.4
PC4 UT-577:   sudo route add default gw 192.168.4.5
PC5 UT-578:   sudo route add default gw 192.168.4.5
```

添加路由规则命令:

```
Router0 U-571: sudo ip route add 192.168.3.0/24 via 192.168.3.4
               sudo ip route add 192.168.2.0/24 via 192.168.2.5
Router1 U-572: sudo ip route add 192.168.4.0/24 via 192.168.4.5
               sudo ip route add 192.168.2.0/24 via 192.168.2.4
```

允许转发命令（在 router1 和 router2 中设置）

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

四、数据包截图

31	37.960946	192.168.3.78	192.168.3.79	ICMP	98 Echo (ping) request	id=0x038d, seq=7/1792, ttl=64
32	37.961313	192.168.3.79	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038d, seq=7/1792, ttl=64
33	38.974846	192.168.3.78	192.168.3.79	ICMP	98 Echo (ping) request	id=0x038d, seq=8/2048, ttl=64
34	38.975181	192.168.3.79	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038d, seq=8/2048, ttl=64
35	39.988907	192.168.3.78	192.168.3.79	ICMP	98 Echo (ping) request	id=0x038d, seq=9/2304, ttl=64
36	39.989242	192.168.3.79	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038d, seq=9/2304, ttl=64
37	41.002629	192.168.3.78	192.168.3.79	ICMP	98 Echo (ping) request	id=0x038d, seq=10/2560, ttl=64
38	41.002881	192.168.3.79	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038d, seq=10/2560, ttl=64
39	42.004324	192.168.3.78	192.168.3.79	ICMP	98 Echo (ping) request	id=0x038d, seq=11/2816, ttl=64
40	42.004680	192.168.3.79	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038d, seq=11/2816, ttl=64

PC1 ping PC2

164	285.668448	192.168.4.81	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038f, seq=8/2048, ttl=62
165	286.667846	192.168.3.78	192.168.4.81	ICMP	98 Echo (ping) request	id=0x038f, seq=9/2304, ttl=64
166	286.669161	192.168.4.81	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038f, seq=9/2304, ttl=62
167	287.669822	192.168.3.78	192.168.4.81	ICMP	98 Echo (ping) request	id=0x038f, seq=10/2560, ttl=64
168	287.671228	192.168.4.81	192.168.3.78	ICMP	98 Echo (ping) reply	id=0x038f, seq=10/2560, ttl=62
169	288.672190	192.168.3.78	192.168.4.81	ICMP	98 Echo (ping) request	id=0x038f, seq=11/2816, ttl=64

PC1 ping PC4

43	23.398601	192.168.4.81	192.168.4.82	ICMP	98 Echo (ping) request	id=0x038b, seq=11/2816, ttl=64
44	23.398909	192.168.4.82	192.168.4.81	ICMP	98 Echo (ping) reply	id=0x038b, seq=11/2816, ttl=64
45	24.412627	192.168.4.81	192.168.4.82	ICMP	98 Echo (ping) request	id=0x038b, seq=12/3072, ttl=64
46	24.413873	192.168.4.82	192.168.4.81	ICMP	98 Echo (ping) reply	id=0x038b, seq=12/3072, ttl=64
47	25.426033	192.168.4.81	192.168.4.82	ICMP	98 Echo (ping) request	id=0x038b, seq=13/3328, ttl=64
48	25.426106	192.168.4.82	192.168.4.81	ICMP	98 Echo (ping) reply	id=0x038b, seq=13/3328, ttl=64
49	26.440617	192.168.4.81	192.168.4.82	ICMP	98 Echo (ping) request	id=0x038b, seq=14/3584, ttl=64

PC4 ping PC5

由此可见，两个子网内部，以及子网之间都能 ping 通，说明网络搭建成功。

五、协议报文分析

1、ping 系主页 cs.nju.edu.cn

数据包概览：

16	16.296708	192.168.189.138	192.168.189.2	DNS	73 Standard query A cs.nju.edu.cn
17	16.297764	192.168.189.2	192.168.189.138	DNS	177 Standard query response CNAME www.nju.edu.cn A 202.119.32.7
18	16.298348	192.168.189.138	202.119.32.7	ICMP	98 Echo (ping) request id=0x0940, seq=1/256, ttl=64
19	16.299368	202.119.32.7	192.168.189.138	ICMP	98 Echo (ping) reply id=0x0940, seq=1/256, ttl=128
20	16.299712	192.168.189.138	192.168.189.2	DNS	85 Standard query PTR 7.32.119.202.in-addr.arpa
21	16.300810	192.168.189.2	192.168.189.138	DNS	247 Standard query response PTR www.nju.edu.cn
22	17.008828	192.168.189.1	192.168.189.255	NBNS	92 Name query NB 055<00>
23	17.300084	192.168.189.138	202.119.32.7	ICMP	98 Echo (ping) request id=0x0940, seq=2/512, ttl=64
24	17.301275	202.119.32.7	192.168.189.138	ICMP	98 Echo (ping) reply id=0x0940, seq=2/512, ttl=128
25	17.301735	192.168.189.138	192.168.189.2	DNS	85 Standard query PTR 7.32.119.202.in-addr.arpa

▶ Frame 16: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)

▶ Ethernet II, Src: Vmware_82:e5:c3 (00:0c:29:82:e5:c3), Dst: Vmware_f5:06:45 (00:50:56:f5:06:45)

▶ Internet Protocol Version 4, Src: 192.168.189.138 (192.168.189.138), Dst: 192.168.189.2 (192.168.189.2)

▶ User Datagram Protocol, Src Port: 22463 (22463), Dst Port: domain (53)

▶ Domain Name System (query)

```
0000  00 50 56 f5 06 45 00 0c 29 82 e5 c3 08 00 45 00  .PV..E.. )....E.
0010  00 3b 00 00 40 00 40 11 3e d4 c0 a8 bd 8a c0 a8  .;..@.@. >.....
0020  bd 02 57 bf 00 35 00 27 51 34 c0 ee 01 00 00 01  ..W..5.' Q4.....
0030  00 00 00 00 00 00 02 63 73 03 6e 6a 75 03 65 64  .....C s.nju.ed
0040  75 02 63 6e 00 00 01 00 01                          u.cn.... .
```

下面对每个数据包分析：

(1) DNS 包

▼ Ethernet II, Src: Vmware_82:e5:c3 (00:0c:29:82:e5:c3), Dst: Vmware_f5:06:45 (00:50:56:f5:06:45)	
▼ Destination: Vmware_f5:06:45 (00:50:56:f5:06:45)	
Address: Vmware_f5:06:45 (00:50:56:f5:06:45)	
.... 0 = IG bit: Individual address (unicast)	
.... 0. = LG bit: Globally unique address (factory default)	
▼ Source: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)	
Address: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)	
.... 0 = IG bit: Individual address (unicast)	
.... 0. = LG bit: Globally unique address (factory default)	
Type: IP (0x0800)	
▼ Internet Protocol Version 4, Src: 192.168.189.138 (192.168.189.138), Dst: 192.168.189.2 (192.168.189.2)	
0000	00 50 56 f5 06 45 00 0c 29 82 e5 c3 08 00 45 00 .PV..E..)....E.
0010	00 3b 00 00 40 00 40 11 3e d4 c0 a8 bd 8a c0 a8 .;..@.@. >.....
0020	bd 02 57 bf 00 35 00 27 51 34 c0 ee 01 00 00 01 ..W..5.' Q4.....
0030	00 00 00 00 00 00 02 63 73 03 6e 6a 75 03 65 64C s.nju.ed
0040	75 02 63 6e 00 00 01 00 01 u.cn.... .

00 50 56 f5 06 45 为目标节点 MAC，

00 0c 29 82 e5 c3 为源节点 MAC，

08 00 表明以太网帧协议为 IP 类型。

45 表示表示当前使用的 IP 版本及数据报协议头长度，

00 表示服务类型，

00 3b 指定整个 IP 数据报的字节长度，

00 00 为标识符，用于识别当前数据报，

40 00 是标志与偏移，

40 表示生存时间，

11 是协议类型，指出在 IP 处理完成后，又哪种上层协议接受导入数据包，这里是指 UDP 协议，

3e 4d 为包头校验码，

c0 a8 bd 8a 为源 IP 地址，
c0 a8 bd 02 为目的 IP 地址。
57 bf 为 UDP 源端口号，
00 35 为 UDP 目的端口号，
00 27 为 UDP 数据报长度，
51 34 为校验码，之后的 c0 ee 01 00 ... 00 01 00 01 为 UDP 数据包的数据区。

(2) ICMP 包

17	16.297764	192.168.189.2	192.168.189.138	DNS	177	Standard query response CM
18	16.298348	192.168.189.138	202.119.32.7	ICMP	98	Echo (ping) request id=0x
19	16.299368	202.119.32.7	192.168.189.138	ICMP	98	Echo (ping) reply id=0x
20	16.299712	192.168.189.138	192.168.189.2	DNS	85	Standard query PTR 7.32.11
21	16.300810	192.168.189.2	192.168.189.138	DNS	247	Standard query response PT
22	17.008828	192.168.189.1	192.168.189.255	NBNS	92	Name query NB 055<00>
23	17.300084	192.168.189.138	202.119.32.7	ICMP	98	Echo (ping) request id=0x
24	17.301275	202.119.32.7	192.168.189.138	ICMP	98	Echo (ping) reply id=0x
25	17.301735	192.168.189.138	192.168.189.2	DNS	85	Standard query PTR 7.32.11


```

[Frame is ignored: False]
[Protocols in frame: eth:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: Vmware_82:e5:c3 (00:0c:29:82:e5:c3), Dst: Vmware_f5:06:45 (00:50:56:f5:06:45)
  ▼ Destination: Vmware_f5:06:45 (00:50:56:f5:06:45)
    Address: Vmware_f5:06:45 (00:50:56:f5:06:45)
      ....0. .... = IG bit: Individual address (unicast)
      ....0. .... = LG bit: Globally unique address (factory default)
  ▼ Source: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)
    Address: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)
      ....0. .... = IG bit: Individual address (unicast)
      ....0. .... = LG bit: Globally unique address (factory default)
  
```


0000	00 50 56 f5 06 45	00 0c 29 82 e5 c3 08 00 45 00	.PV..E..)....E.
0010	00 54 00 00 40 00 40 01	d1 f7 c0 a8 bd 8a ca 77	.T..@. @.w
0020	20 07 08 00 65 c0 09 40	00 01 26 f3 b7 58 b3 af	...e..@ ..&..X..
0030	0c 00 08 09 0a 0b 0c 0d	0e 0f 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25!"#\$%
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,- ./012345
0060	36 37		67

00 50 56 f5 06 45 为目标节点 MAC，
00 0c 29 82 e5 c3 为源节点 MAC，
08 00 表明以太网帧协议为 IP 类型。
45 表示表示当前使用的 IP 版本及数据报协议头长度，
00 表示服务类型，
00 54 指定整个 IP 数据报的字节长度，
00 00 为标识符，用于识别当前数据报，
40 00 是标志与偏移，
40 表示生存时间，
01 是协议类型，这里是指 ICMP 协议，
d1 f7 为包头校验码，
c0 a8 bd 8a 为源 IP 地址，
ca 77 20 07 为目的 IP 地址。
08 是指消息类型，这里是指 request，
00 为代码，
65 c0 为 ICMP 校验码，
09 40 为 ICMP 标识符，

00 01 为序列号，
26 f3 b7 58 ... 34 35 36 37 为数据区。

2、用浏览器访问 www.nju.edu.cn

数据包概览：

2	11.282475	192.168.189.138	192.168.189.2	DNS	74 Standard query A www.nju.edu.
3	11.284436	Vmware_f5:06:45	Broadcast	ARP	60 Who has 192.168.189.138? Tel
4	11.284453	Vmware_82:e5:c3	Vmware_f5:06:45	ARP	42 192.168.189.138 is at 00:0c:2
5	11.284703	192.168.189.2	192.168.189.138	DNS	346 Standard query response A 202
6	11.302634	192.168.189.138	202.119.32.7	TCP	74 45194 > http [SYN] Seq=0 Win=
7	11.304123	202.119.32.7	192.168.189.138	TCP	60 http > 45194 [SYN, ACK] Seq=0
8	11.304157	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=1 Ack=
9	11.304558	192.168.189.138	202.119.32.7	HTTP	344 GET / HTTP/1.1
10	11.304931	202.119.32.7	192.168.189.138	TCP	60 http > 45194 [ACK] Seq=1 Ack=
11	11.308616	202.119.32.7	192.168.189.138	TCP	300 [TCP segment of a reassembled
12	11.308642	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=291 Ac
13	11.513379	202.119.32.7	192.168.189.138	TCP	1514 [TCP segment of a reassembled
14	11.513411	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=291 Ac
15	11.513475	202.119.32.7	192.168.189.138	TCP	1514 [TCP segment of a reassembled
16	11.513483	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=291 Ac
17	11.513519	202.119.32.7	192.168.189.138	TCP	1514 [TCP segment of a reassembled
18	11.513525	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=291 Ac
19	11.513558	202.119.32.7	192.168.189.138	TCP	1514 [TCP segment of a reassembled
20	11.513564	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK] Seq=291 Ac

可以看出，与 ping 相比，这里多出来 ARP，TCP，HTTP 这三种协议包，下面对这三种协议包的内容进行解析。

(3) ARP 包

2	11.282475	192.168.189.138	192.168.189.2	DNS	74 Standard c
3	11.284436	Vmware_f5:06:45	Broadcast	ARP	60 Who has 19
4	11.284453	Vmware_82:e5:c3	Vmware_f5:06:45	ARP	42 192.168.18
5	11.284703	192.168.189.2	192.168.189.138	DNS	346 Standard c
6	11.302634	192.168.189.138	202.119.32.7	TCP	74 45194 > ht
7	11.304123	202.119.32.7	192.168.189.138	TCP	60 http > 451
8	11.304157	192.168.189.138	202.119.32.7	TCP	54 45194 > ht
9	11.304558	192.168.189.138	202.119.32.7	HTTP	344 GET / HTTP
10	11.304931	202.119.32.7	192.168.189.138	TCP	60 http > 451

▶ Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)					
▼ Ethernet II, Src: Vmware_f5:06:45 (00:50:56:f5:06:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)					
Address: Broadcast (ff:ff:ff:ff:ff:ff)					
.... 1 = IG bit: Group address (multicast/broadcast)					
.... 1. = LG bit: Locally administered address (this is NOT the)					
▼ Source: Vmware_f5:06:45 (00:50:56:f5:06:45)					
Address: Vmware_f5:06:45 (00:50:56:f5:06:45)					
.... 0 = IG bit: Individual address (unicast)					
.... 0. = LG bit: Globally unique address (factory default)					
Type: ARP (0x0806)					
Trailer: 00000000000000000000000000000000					
▼ Address Resolution Protocol (request)					
Hardware type: Ethernet (1)					
0000	ff ff ff ff ff ff	00 50	56 f5 06 45 08 06 00 01	P V..E....
0010	08 00 06 04 00 01	00 50	56 f5 06 45 c0 a8 bd 02	P V..E....
0020	00 00 00 00 00 00	c0 a8	bd 8a 00 00 00 00 00 00
0030	00 00 00 00 00 00	00 00	00 00 00 00

ff ff ff ff ff ff 表示广播地址，
 00 50 56 f5 06 45 为源 MAC 地址，
 08 06 是协议类型，这里表示 ARP 协议。
 00 01 是硬件类型：指明了发送方想知道的硬件接口类型，以太网的值为 1，
 08 00 是协议类型：指明了发送方提供的高层协议类型，
 IP 为 0800（16 进制），
 06 是指硬件地址长度，
 04 是指协议长度，
 00 01 表示操作类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4，
 00 50 56 f5 06 45 为发送者 MAC，
 c0 a8 bd 02 为发送者 IP，
 00 00 00 00 00 00 为目标 MAC，
 c0 a8 bd 8a 为目标 IP。

(1) TCP 包

6	11.302634	192.168.189.138	202.119.32.7	TCP	74 45
7	11.304123	202.119.32.7	192.168.189.138	TCP	60 ht
8	11.304157	192.168.189.138	202.119.32.7	TCP	54 45
9	11.304558	192.168.189.138	202.119.32.7	HTTP	344 GE
10	11.304931	202.119.32.7	192.168.189.138	TCP	60 ht

▶ Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▼ Ethernet II, Src: Vmware_f5:06:45 (00:50:56:f5:06:45), Dst: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)

▼ Destination: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)

Address: Vmware_82:e5:c3 (00:0c:29:82:e5:c3)

.... 0 = IG bit: Individual address (unicast)
 0 = LG bit: Globally unique address (factory default)

▼ Source: Vmware_f5:06:45 (00:50:56:f5:06:45)

Address: Vmware_f5:06:45 (00:50:56:f5:06:45)

.... 0 = IG bit: Individual address (unicast)
 0 = LG bit: Globally unique address (factory default)

Type: IP (0x0800)
 Trailer: 0000

▼ Internet Protocol Version 4, Src: 202.119.32.7 (202.119.32.7), Dst: 192.168.189.138

0000	00 0c 29 82 e5 c3	00 50 56 f5 06 45 08 00 45 00	..).P V..E..E.
0010	00 2c ff 8f 00 00 80 06	d2 8a ca 77 20 07 c0 a8w...
0020	bd 8a 00 50 b0 8a 79 11	1c 26 37 a8 d8 e5 60 12	...P.y. &7...
0030	fa f0 dd d3 00 00 02 04	05 b4 00 00

00 0c 29 82 e5 c3 为目的 MAC 地址，
 00 50 56 f5 06 45 为源 MAC 地址，
 08 00 为协议类型（IP），
 45 表示表示当前使用的 IP 版本及数据报协议头长度，
 00 表示服务类型，
 00 2c 指定整个 IP 数据报的字节长度，
 ff 8f 为标识符，用于识别当前数据报，

00 00 是标志与偏移，
80 表示生存时间，
06 是协议类型，这里是指 TCP 协议，
d2 8a 为包头校验码，
ca 77 20 07 为源 IP 地址，
c0 a8 bd 8a 为目的 IP 地址。
00 50 b0 ... b4 为 TCP 负载数据。其中：00 50 是指 TCP 源端口号，b0 8a 为 TCP 目的端口号，79 11 1c 26 为序列号，37 a8 d8 e5 为确认号。

(1) HTTP 包

7	11.304125	202.119.32.7	192.168.189.138	TCP	60 http > 45194 [STN,
8	11.304157	192.168.189.138	202.119.32.7	TCP	54 45194 > http [ACK]
9	11.304558	192.168.189.138	202.119.32.7	HTTP	344 GET / HTTP/1.1
10	11.304931	202.119.32.7	192.168.189.138	TCP	60 http > 45194 [ACK]

```

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length: 330
Identification: 0x92a9 (37545)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x3e53 [fragment]
0 00 50 56 f5 06 45 00 0c 29 82 e5 c3 08 00 45 00 .PV..E.. )....E.
0 01 4a 92 a9 40 00 40 06 3e 53 c0 a8 bd 8a ca 77 .J..@.@. >S....w
0 20 07 b0 8a 00 50 37 a8 d8 e5 79 11 1c 27 50 18 ....P7. .y..'P.
0 39 08 93 45 00 00 47 45 54 20 2f 20 48 54 54 50 9..E..GE T / HTTP
0 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Host: www.
0 6e 6a 75 2e 65 64 75 2e 63 6e 0d 0a 55 73 65 72 nju.edu. cn..User
0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0 35 2e 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 5.0 (X11 ; Ubuntu
0 3b 20 4c 69 6e 75 78 20 69 36 38 36 3b 20 72 76 ; Linux i686; rv
0 3a 31 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 :11.0) Gecko/201
0 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 31 00101 Firefox/11
0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 . Accept: text

```

这个包的 IP 报头和 TCP 的 IP 报头基本一致，可以看出该报头中使用的协议类型仍然是 TCP 协议。

```

Destination port: http (80)
[Stream index: 2]
Sequence number: 1 (relative sequence number)
[Next sequence number: 291 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
000 00 50 56 f5 06 45 00 0c 29 82 e5 c3 08 00 45 00 .
010 01 4a 92 a9 40 00 40 06 3e 53 c0 a8 bd 8a ca 77 .
020 20 07 b0 8a 00 50 37 a8 d8 e5 79 11 1c 27 50 18
030 30 08 93 45 00 00 47 45 54 20 2f 20 48 54 54 50

```

在包中可以看到目的端口是 80，所以该报文的目标是浏览器。

▼ Hypertext Transfer Protocol

▼ GET / HTTP/1.1\r\n

▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: www.nju.edu.cn\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:11.0) Gecko/20100101 Firefox/11.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-us,en;q=0.5\r\n

0000	00 50 56 f5 06 45 00 0c 29 82 e5 c3 08 00 45 00	.PV..E..).....E.
0010	01 4a 92 a9 40 00 40 06 3e 53 c0 a8 bd 8a ca 77	.J..@.@. >S.....w
0020	20 07 b0 8a 00 50 37 a8 d8 e5 79 11 1c 27 50 18P7. ..y..'P.
0030	39 08 93 45 00 00 47 45 54 20 2f 20 48 54 54 50	9..E..GET / HTTP

在包中还包括有关 http 的其他信息，比如请求方法（GET），user-agent 等等。