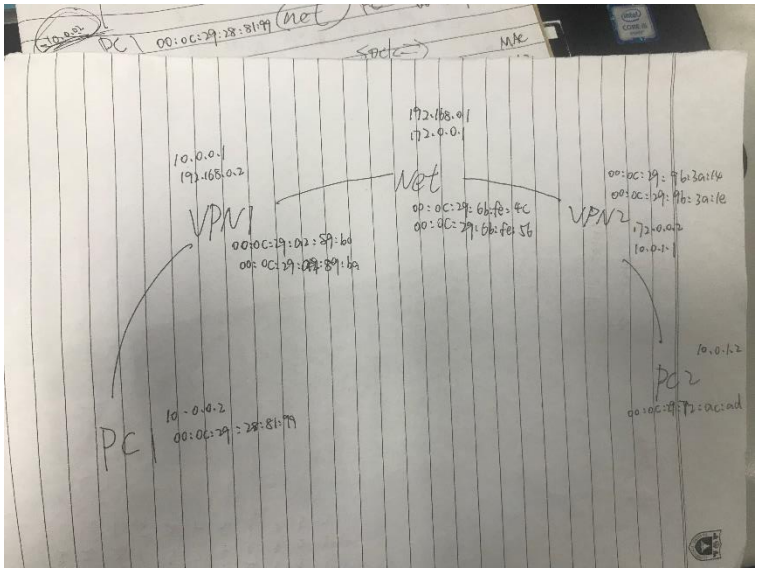
实验六 VPN 设计、实现与分析

李杨 161220071

实验目标

本实验主要目的是设计和实现一个简单的虚拟专用网络的机制，并与已有的标准实现（如 PPTP）进行比较，进而让学生进一步理解 VPN 的工作原理和内部实现细节。

拓扑图:



数据结构:

```
    struct route_item               //route item
{
    char destination[16];        //目的 ip
    char gateway[16];        //网关
    char netmask[16];        //掩码
    int interface;                  //接口
```

```
}route_info[ROUTE_INFO_MAX];
int route_item_index=0;

struct arp_table_item
{
    char ip_addr[16];          //掩码 IP
    char mac_addr[18];      //下一跳 MAC 地址
}arp_table[ARP_SIZE_MAX];
int arp_item_index=0;

struct device_info
{
    char mac[18];              //本地 MAC
    int interface;          //本地接口
    //int is_entrance;
}device[DEVICE_MAX];
```

其余的结构体如 ip,sockaddr 为调用库函数。

网络配置：

PC1:

```
root@ubuntu:/home/user# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:81:99
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:8199/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1277 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23129 (23.1 KB)  TX bytes:184441 (184.4 KB)
          Interrupt:19 Base address:0x2000
```

VPN1:

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a2:89:b0
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea2:89b0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8061 errors:0 dropped:0 overruns:0 frame:0
          TX packets:447 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:781246 (781.2 KB)  TX bytes:42777 (42.7 KB)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:a2:89:ba
          inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea2:89ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:348 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35731 (35.7 KB)  TX bytes:1470618 (1.4 MB)
```

NETWORK:

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6b:fe:4c
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6b:fe4c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7799 errors:0 dropped:0 overruns:0 frame:0
          TX packets:295 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:813424 (813.4 KB)  TX bytes:30287 (30.2 KB)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:6b:fe:56
          inet addr:172.0.0.1  Bcast:172.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6b:fe56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:393 errors:0 dropped:0 overruns:0 frame:0
          TX packets:145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:48494 (48.4 KB)  TX bytes:23286 (23.2 KB)
          Interrupt:19 Base address:0x2080
          ^C
```

VPN2:

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9b:3a:14
          inet addr:172.0.0.2  Bcast:172.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9b:3a14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5206 (5.2 KB)  TX bytes:163159 (163.1 KB)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:9b:3a:1e
          inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9b:3a1e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:832 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:80418 (80.4 KB)  TX bytes:25278 (25.2 KB)
          Interrupt:19 Base address:0x2080
```

PC2:

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:72:ac:ad
          inet addr:10.0.1.2  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe72:acad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:316 errors:0 dropped:0 overruns:0 frame:0
          TX packets:921 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:57944 (57.9 KB)  TX bytes:95927 (95.9 KB)
          Interrupt:19 Base address:0x2000
```

实验设计思路:

一个标准的 ip 包，其内容未知，包头地址为 vpn 的地址，发送到 vpn 的接入口后，包被解析，对包中的 ip 地址与本地的 arp 表中保存的 IP 地址进行比较分析，如果本地的 arp 表中有与之相同的，则说明找到了要发往的具体的地方，则发送给 arp 表中所搜到的 ip 对应的 mac 地址，否则的话则重新发回网络。在两个 vpn 之间传输的时候，会有 rapack 和 unpack 操作，也就是在一开始收到包并解析后，在包的头部加上必要的信息，然后将内容打包成一个 ip 包，并发往

网络进行传输。

实验结果:

PC1 ping pc2

```
user@ubuntu:~$ ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
64 bytes from 10.0.1.2: icmp_req=1 ttl=64 time=5.40 ms
64 bytes from 10.0.1.2: icmp_req=2 ttl=64 time=6.32 ms
64 bytes from 10.0.1.2: icmp_req=3 ttl=64 time=5.01 ms
64 bytes from 10.0.1.2: icmp_req=4 ttl=64 time=4.46 ms
64 bytes from 10.0.1.2: icmp_req=5 ttl=64 time=4.13 ms
64 bytes from 10.0.1.2: icmp_req=6 ttl=64 time=3.02 ms
64 bytes from 10.0.1.2: icmp_req=7 ttl=64 time=2.99 ms
64 bytes from 10.0.1.2: icmp_req=8 ttl=64 time=3.24 ms
^C
--- 10.0.1.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 2.992/4.325/6.328/1.140 ms
```

Wireshark

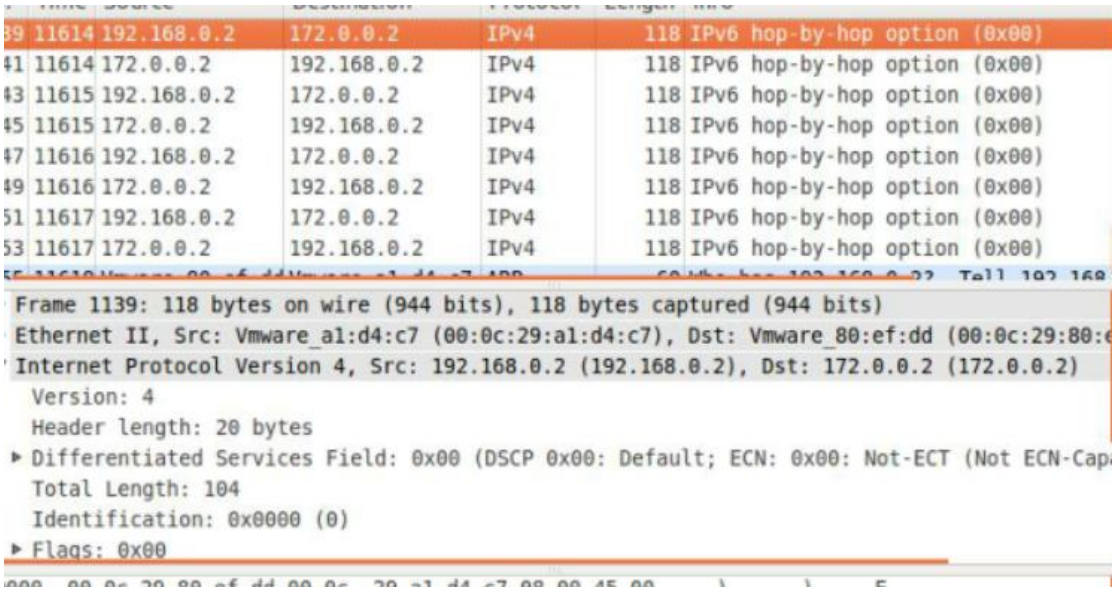
Pc0 上的 eth0

```
11428 10.0.1.2  10.0.0.2  ICMP  98 Echo (ping) reply    id=0x0b40, seq=1/256, ttl=
11429 10.0.0.2  10.0.1.2  ICMP  98 Echo (ping) request  id=0x0b40, seq=2/512, ttl=
11429 10.0.1.2  10.0.0.2  ICMP  98 Echo (ping) reply    id=0x0b40, seq=2/512, ttl=
11430 10.0.0.2  10.0.1.2  ICMP  98 Echo (ping) request  id=0x0b40, seq=3/768, ttl=
11430 10.0.1.2  10.0.0.2  ICMP  98 Echo (ping) reply    id=0x0b40, seq=3/768, ttl=
11431 10.0.0.2  10.0.1.2  ICMP  98 Echo (ping) request  id=0x0b40, seq=4/1024, ttl
11431 10.0.1.2  10.0.0.2  ICMP  98 Echo (ping) reply    id=0x0b40, seq=4/1024, ttl
11432 10.0.0.2  10.0.1.2  ICMP  98 Echo (ping) request  id=0x0b40, seq=5/1280, ttl
11432 10.0.1.2  10.0.0.2  ICMP  98 Echo (ping) reply    id=0x0b40, seq=5/1280, ttl

▸ Frame 310: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: Vmware_a1:d4:bd (00:0c:29:a1:d4:bd), Dst: Vmware_f0:7e:33 (00:0c:29:f0
▾ Internet Protocol Version 4, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.0.2 (10.0.0.2)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Ca
    Total Length: 84

0000  00 0c 29 f0 7e 33 00 0c  29 a1 d4 bd 08 00 45 00   ..).~3.. ).....E.
0010  00 54 a1 f0 00 00 40 01  c3 b5 0a 00 01 02 0a 00   .T....@. ........
0020  00 02 00 00 28 44 0b 40  00 02 fe 21 2a 5b ad f9   ....(D.@ ...!*[..
0030  0b 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
```

Vpn1:



39	11614	192.168.0.2	172.0.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
41	11614	172.0.0.2	192.168.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
43	11615	192.168.0.2	172.0.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
45	11615	172.0.0.2	192.168.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
47	11616	192.168.0.2	172.0.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
49	11616	172.0.0.2	192.168.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
51	11617	192.168.0.2	172.0.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)
53	11617	172.0.0.2	192.168.0.2	IPv4	118	IPv6 hop-by-hop option (0x00)

```
Frame 1139: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: Vmware_a1:d4:c7 (00:0c:29:a1:d4:c7), Dst: Vmware_80:ef:dd (00:0c:29:80:e
Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 172.0.0.2 (172.0.0.2)
  Version: 4
  Header length: 20 bytes
▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Cap
  Total Length: 104
  Identification: 0x0000 (0)
▸ Flags: 0x00
```

当关闭 vpn：

```
root@ubuntu:/home/user# ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
```