

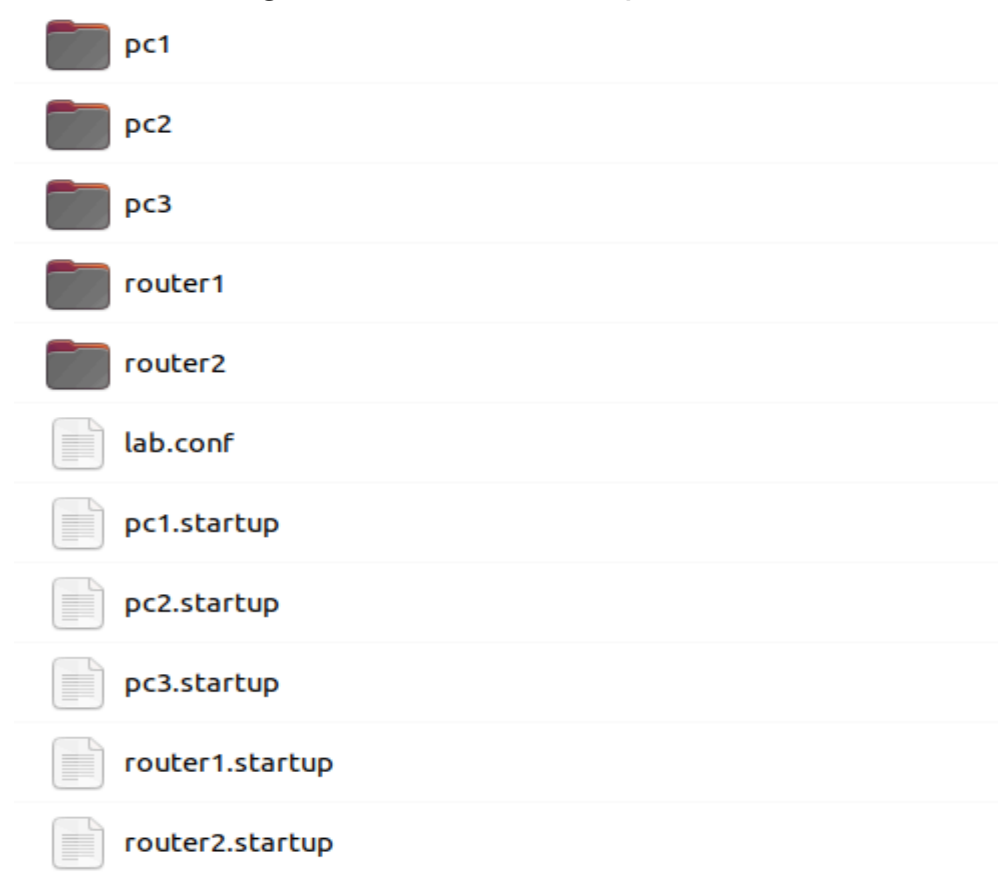
Buổi thực hành 2

Huỳnh Quốc Dinh
B2110009

BÀI TẬP 5: Mô phỏng mạng ảo như hình phía dưới, cài đặt bảng vạch đường tĩnh và khảo sát giao thức ICMP bằng Wireshark

Bước 1: Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

Bước 2: Xây dựng cấu trúc thư mục mạng ảo (nằm dưới thư mục cá nhân /home/student<mã số sinh viên>) với đầy đủ các thư mục con và các file cấu hình (.startup, lab.conf). Thư mục mạng ảo đặt tên là BaiTap5



Bước 3: Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

```
lab.conf
~/b2110009/baitap5

1 pc1[0]=A
2 pc2[0]=B
3 pc3[0]=C
4 router1[0]=A
5 router1[1]=B
6 router2[0]=A
7 router2[1]=C
```

Bước 4: Trên file PC1.startup, thông tin vạch đường đến LAN B và C được bổ sung vào bảng vạch đường của PC1 như sau

```
GNU nano 6.2 pc1.startup
ifconfig eth0 10.0.0.101/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
route add -net 10.0.2.0/24 gw 10.0.0.2
```

Bước 5: Thực hiện tương tự trên PC2.startup (kết nối đến LAN A và LAN C)

```
GNU nano 6.2 pc2.startup
ifconfig eth0 10.0.1.101/24 up
route add -net 10.0.0.0/24 gw 10.0.1.1
route add -net 10.0.2.0/24 gw 10.0.1.1
```

```
GNU nano 6.2 pc3.startup
ifconfig eth0 10.0.2.101/24 up
route add -net 10.0.0.0/24 gw 10.0.2.1
route add -net 10.0.1.0/24 gw 10.0.2.1
```

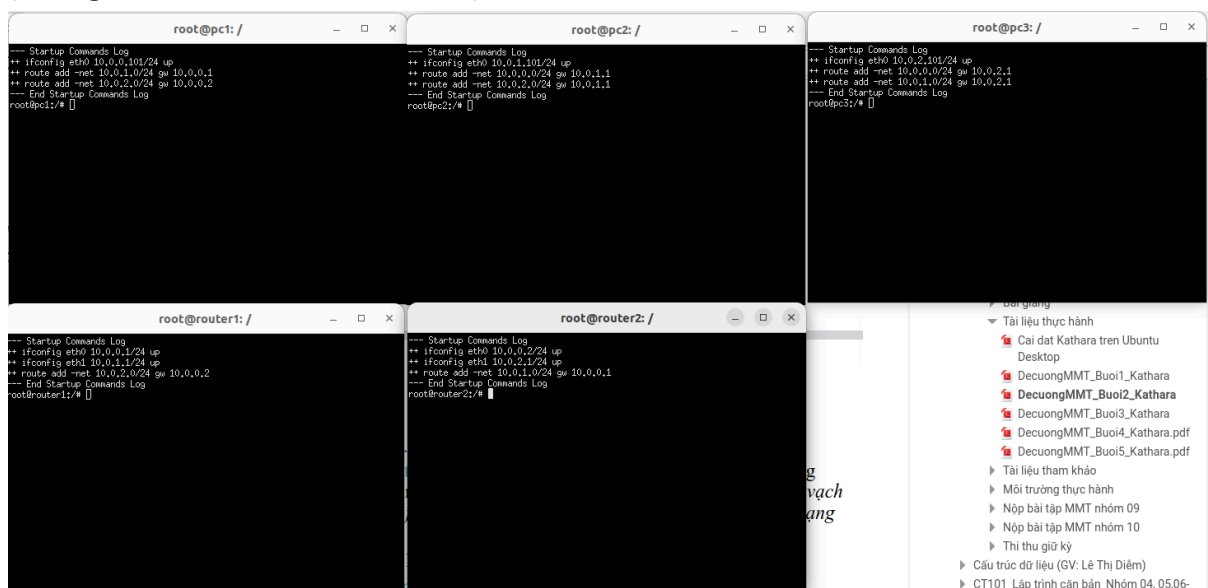
Bước 6: Thêm thông tin vạch đường trên Router1.startup và Router2.startup bằng lệnh route add -net đã được hướng dẫn sao cho Router1 biết đường đi tới LAN C và Router 2 biết đường đi tới LAN B.

Nội dung file Router1.startup có thể được trình bày như sau:
Thực hiện tương tự cho Router2.startup của Router2

```
GNU nano 6.2 router1.startup
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.1.1/24 up
route add -net 10.0.2.0/24 gw 10.0.0.2
```

```
GNU nano 6.2 router2.startup
ifconfig eth0 10.0.0.2/24 up
ifconfig eth1 10.0.2.1/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
```

Bước 7: Khởi động mạng ảo BaiTap5 (bằng lệnh `kathara lstart`). Kiểm tra các cấu hình IP và các bảng vạch đường (bằng lệnh `ifconfig` và `route`) trên từng router và pc. Lưu ý: Nếu cấu hình IP hoặc/và bảng vạch đường của 1 thiết bị nào đó bị sai, điều chỉnh lại các file cấu hình (**.startup**, **lab.conf**) và khởi động lại mạng ảo (bằng lệnh `kathara lrestart`).



Bước 8: Trên PC2, Router1 và Router2 lần lượt thực hiện lệnh `tcpdump` với cú pháp

```
root@router1: /  
--- Startup Commands Log  
++ ifconfig eth0 10.0.0.1/24 up  
++ ifconfig eth1 10.0.1.1/24 up  
++ route add -net 10.0.2.0/24 gw 10.0.0.2  
--- End Startup Commands Log  
root@router1:/# tcpdumb -s 1536 -w /shared/BTH5_router1.pcap  
bash: tcpdumb: command not found  
root@router1:/# tcpdumb -s 1536 -w /shared/BTH5_router1.pcap  
bash: tcpdumb: command not found  
root@router1:/# tcpdumb -s 1536 -w /shared/BTH5_Router1.pcap  
bash: tcpdumb: command not found  
root@router1:/# tcpdumb -s 1536 -w /shared/BTH5_router1.pcap  
bash: tcpdumb: command not found  
root@router1:/# tcpdumb -s 1536 -w /shared/BTH5_router1.pcap  
bash: tcpdumb: command not found  
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 by  
tes  
█
```

```
root@pc2: /  
--- Startup Commands Log  
++ ifconfig eth0 10.0.1.101/24 up  
++ route add -net 10.0.0.0/24 gw 10.0.1.1  
++ route add -net 10.0.2.0/24 gw 10.0.1.1  
--- End Startup Commands Log  
root@pc2:/# tcpdump -s 1536 -w /shared/BTH5_PC2.pcap  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 by  
tes  
█
```

```
root@router2: /
--- Startup Commands Log
+ ifconfig eth0 10.0.0.2/24 up
+ ifconfig eth1 10.0.2.1/24 up
+ route add -net 10.0.1.0/24 gw 10.0.0.1
--- End Startup Commands Log
root@router2:/# tcpdump -s 1536 -w /shared/BTH5_router2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
```

.Bước 9:Trên PC3 thực hiện lệnh ping đến PC2 (ping 10.0.1.101) và chờ khoảng 10 giây. Sau đó dừng lệnh ping trên PC3 và các các lệnh tcpdump trên PC2, Router1 và Router2 (gõ tổ hợp phím Ctrl C)

```
root@pc3: /
64 bytes from 10.0.1.101: icmp_seq=112 ttl=62 time=1.32 ms
64 bytes from 10.0.1.101: icmp_seq=113 ttl=62 time=1.36 ms
64 bytes from 10.0.1.101: icmp_seq=114 ttl=62 time=1.37 ms
64 bytes from 10.0.1.101: icmp_seq=115 ttl=62 time=1.42 ms
64 bytes from 10.0.1.101: icmp_seq=116 ttl=62 time=1.44 ms
top
64 bytes from 10.0.1.101: icmp_seq=117 ttl=62 time=1.45 ms
64 bytes from 10.0.1.101: icmp_seq=118 ttl=62 time=1.42 ms
64 bytes from 10.0.1.101: icmp_seq=119 ttl=62 time=1.28 ms
64 bytes from 10.0.1.101: icmp_seq=120 ttl=62 time=1.43 ms
64 bytes from 10.0.1.101: icmp_seq=121 ttl=62 time=1.24 ms
64 bytes from 10.0.1.101: icmp_seq=122 ttl=62 time=1.37 ms
64 bytes from 10.0.1.101: icmp_seq=123 ttl=62 time=1.20 ms
64 bytes from 10.0.1.101: icmp_seq=124 ttl=62 time=1.44 ms
64 bytes from 10.0.1.101: icmp_seq=125 ttl=62 time=1.09 ms
64 bytes from 10.0.1.101: icmp_seq=126 ttl=62 time=1.46 ms
64 bytes from 10.0.1.101: icmp_seq=127 ttl=62 time=1.34 ms
64 bytes from 10.0.1.101: icmp_seq=128 ttl=62 time=1.41 ms
64 bytes from 10.0.1.101: icmp_seq=129 ttl=62 time=1.19 ms
^C
--- 10.0.1.101 ping statistics ---
129 packets transmitted, 129 received, 0% packet loss, time 128488ms
rtt min/avg/max/mdev = 0.337/1.269/1.842/0.285 ms
root@pc3:/#
```

```
root@pc2: /
--- Startup Commands Log
++ ifconfig eth0 10.0.1.101/24 up
++ route add -net 10.0.0.0/24 gw 10.0.1.1
++ route add -net 10.0.2.0/24 gw 10.0.1.1
--- End Startup Commands Log
root@pc2:/# tcpdump -s 1536 -w /shared/BTH5_PC2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C276 packets captured
276 packets received by filter
0 packets dropped by kernel
root@pc2:/#

root@router2: /
--- Startup Commands Log
++ ifconfig eth0 10.0.0.2/24 up
++ ifconfig eth1 10.0.2.1/24 up
++ route add -net 10.0.1.0/24 gw 10.0.0.1
--- End Startup Commands Log
root@router2:/# tcpdump -s 1536 -w /shared/BTH5_router2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C274 packets captured
274 packets received by filter
0 packets dropped by kernel
root@router2:/#

root@router1: /
--- Startup Commands Log
++ ifconfig eth0 10.0.0.1/24 up
++ ifconfig eth1 10.0.1.1/24 up
++ route add -net 10.0.2.0/24 gw 10.0.0.2
--- End Startup Commands Log
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap
bash: tcpdump: command not found
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap
bash: tcpdump: command not found
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_Router1.pcap
bash: tcpdump: command not found
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap
bash: tcpdump: command not found
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap
bash: tcpdump: command not found
root@router1:/# tcpdump -s 1536 -w /shared/BTH5_router1.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C274 packets captured
274 packets received by filter
0 packets dropped by kernel
root@router1:/#
```

Bước 10: Trên máy thực Ubuntu, dùng Wireshark mở các file BT5_PC2.pcap (nằm trong thư mục BaiTap5/shared), chọn khung vật lý (frame) số 3 (là khung ICMP đầu tiên, như hình bên dưới)

| BTH5_router2.pcap | | | | | | |
|--|----------|-------------------|-------------------|----------|--------|-----------------------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | | |
| Apply a display filter ... <Ctrl-/> | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1 | 0.000000 | 42:e0:01:6e:31:ee | Broadcast | ARP | 42 | Who has 10.0.0.1? Tel |
| 2 | 0.000380 | 3e:0d:19:4d:b3:bc | 42:e0:01:6e:31:ee | ARP | 60 | 10.0.0.1 is at 3e:0d: |
| 3 | 0.000383 | 10.0.2.101 | 10.0.1.101 | ICMP | 98 | Echo (ping) request |
| 4 | 0.000749 | 10.0.1.101 | 10.0.2.101 | ICMP | 98 | Echo (ping) reply |
| 5 | 1.001193 | 10.0.2.101 | 10.0.1.101 | ICMP | 98 | Echo (ping) request |
| 6 | 1.002112 | 10.0.1.101 | 10.0.2.101 | ICMP | 98 | Echo (ping) reply |
| 7 | 2.002892 | 10.0.2.101 | 10.0.1.101 | ICMP | 98 | Echo (ping) request |
| 8 | 2.003832 | 10.0.1.101 | 10.0.2.101 | ICMP | 98 | Echo (ping) reply |
| 9 | 3.004613 | 10.0.2.101 | 10.0.1.101 | ICMP | 98 | Echo (ping) request |
| 10 | 3.005533 | 10.0.1.101 | 10.0.2.101 | ICMP | 98 | Echo (ping) reply |

▶ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 ▶ Ethernet II, Src: 42:e0:01:6e:31:ee (42:e0:01:6e:31:ee), Dst: 3e:0d:19:4d:b3:bc (3e:0d:19:4d:b3:bc)
 ▶ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
 ▶ Internet Control Message Protocol

| | | |
|------|---|--------------------|
| 0000 | 3e 0d 19 4d b3 bc 42 e0 01 6e 31 ee 08 00 45 00 | >...M..B..n1...E.. |
| 0010 | 00 54 6b c5 40 00 3f 01 b8 1a 0a 00 02 65 0a 00 | ..Tk.@.?.....e.. |
| 0020 | 01 65 08 00 8b c7 00 01 00 01 d2 0e f4 65 00 00 | ..e.....e.. |
| 0030 | 00 00 da ee 0c 00 00 00 00 00 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 |

BTH5_router2.pcap Packets: 274 - Displayed: 274 (100.0%) Profile: Default

Câu hỏi 1:

- Toàn bộ khung số 3 có kích thước là bao nhiêu (Bytes)?

Trả lời: 98 Bytes (gồm 14 bytes header Ethernet và 84 bytes payload)

- Chọn Header Internet Control Message Protocol trong khung và cho biết:

o Gói tin này sử dụng giao thức gì? Giao thức này hoạt động trên tầng nào của mô hình OSI?

Tra lại:

- Gói tin sử dụng giao thức ICMP. Hoạt động trên tầng mạng trong mô hình OSI

o Thông điệp của giao thức này là gì? Thông điệp này có độ dài bao nhiêu (bytes)?

- Các thông điệp của giao thức được gửi đi trong các gói tin IP và được sử dụng để gửi các báo lỗi hay các thông tin điều khiển. Giao thức

thường được các router sử dụng để kiểm tra các host hoặc các router có tồn tại hay không. Có độ dài 48 bytes

- Chọn Header Internet Protocol Version 4 và cho biết:

o Địa chỉ IP của máy gửi dữ liệu là bao nhiêu? Địa chỉ IP này là của máy tính nào trong mạng?

Trả lời:

- Địa chỉ IP của máy gửi dữ liệu là:
- Địa chỉ IP này là của máy tính
⇒ Máy gửi: 10.0.1.101 của pc2

o Địa chỉ IP của máy nhận dữ liệu là bao nhiêu? Địa chỉ IP này là của máy tính nào trong mạng?

- Địa chỉ IP của máy nhận dữ liệu là bao nhiêu
- Địa chỉ IP này là của máy tính
⇒ Máy nhận: 10.0.2.101 của pc3

o Định danh (ID) của gói tin IP này là bao nhiêu (dạng Hexadecimal). Định danh của 1 gói tin có ý nghĩa gì trong thông điệp IP?

Trả lời:

0x22b3, chỉ mã số của 1 IP Datagram, giúp bên nhận có thể ghép các mảnh của 1 IP Datagram lại với nhau vì IP Datagram phân thành các mảnh và các mảnh

thuộc cùng 1 IP Datagram sẽ có cùng Identification.

o Độ dài phần Header của thông điệp IP là bao nhiêu? Phần Header bao gồm những trường nào?

Mỗi trường có độ dài bao nhiêu (Bytes)

- Phần header có độ dài 20 bytes

- Các trường: Version (4 bit), IP Header Length (IHL) (4 bit), Type Of Services (TOS) (8 bit), Total Length (16 bit), Identification (16 bit), Flag (3 bit), Fragment Offset

(13 bit), Time To Live (TTL) (8 bit), Protocol (8 bit), Header CheckSum (16 bit), Source IP

Address (32 bit), Destination IP Address (32 bit), và còn các trường option data có kích thước không cố định

⇒ Header Length là 20 bytes

o Trường Total Length có độ dài là bao nhiêu (Bytes). Hãy lý giải tại sao có độ dài như vậy?

- Chọn Header Ethernet II và cho biết:

```
▼ Ethernet II, Src: 42:e0:01:6e:31:ee (42:e0:01:6e:31:ee), Dst: 3e:0d:19:4d:b3:b6
  ▼ Destination: 3e:0d:19:4d:b3:bc (3e:0d:19:4d:b3:bc)
    Address: 3e:0d:19:4d:b3:bc (3e:0d:19:4d:b3:bc)
    ....1. .... = LG bit: Locally administered address (this
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: 42:e0:01:6e:31:ee (42:e0:01:6e:31:ee)
    Address: 42:e0:01:6e:31:ee (42:e0:01:6e:31:ee)
    ....1. .... = LG bit: Locally administered address (this
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
▼ Internet Control Message Protocol
```

o Địa chỉ MAC của máy gửi dữ liệu là bao nhiêu? Có phải là địa chỉ MAC của máy tính có địa chỉ IP (source) đã tìm được trong câu trên không? Nếu không, hãy lý giải và cho biết địa chỉ MAC này là của máy tính nào trong mạng?

Trả lời:

42:e0:01:6e:31:ee, không phải địa chỉ MAC của máy gửi ở câu trên, địa chỉ này của Router1 trong mạng.

o Địa chỉ MAC của máy nhận dữ liệu là bao nhiêu? Có phải là địa chỉ MAC của máy tính có địa chỉ IP (destination) đã tìm được trong câu trên không? Nếu không, hãy lý giải và cho biết địa chỉ MAC này là của máy tính nào trong mạng?

Trả lời:

- 3e:0d:19:4d:b3:b6, là địa chỉ MAC của máy nhận ở câu trên.

o Trường Type mang giá trị (Hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?

Trả lời:

0x0800 thể hiện ipv4

o Hãy chỉ ra trường Payload của khung Ethernet II? Trường Payload này có độ dài bằng bao nhiêu (Bytes)?

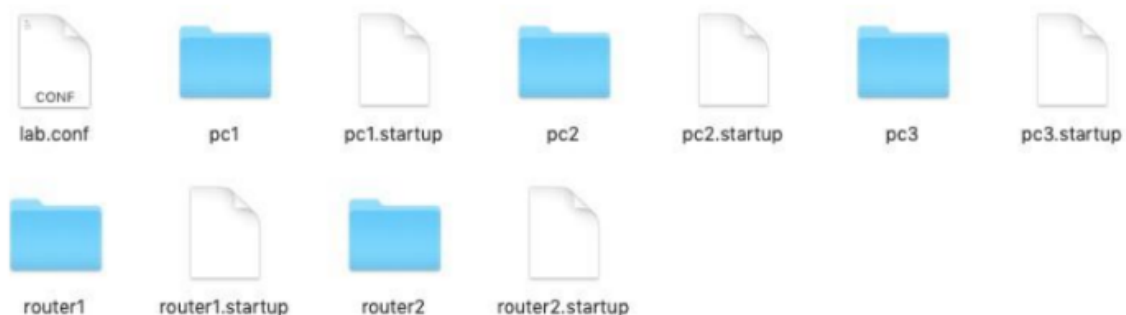
Trả lời:

- Trường payload của khung Ethernet bao gồm phần data chứa phần header và data (Phần giao thức tcp/udp) của giao thức IP có độ dài 84bytes.

BÀI TẬP 6: Vạch đường tĩnh và gói tin ARP

Bước 1: Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

Bước 2: Xây dựng cấu trúc thư mục mạng ảo (nằm dưới thư mục cá nhân /home/student) với đầy đủ các thư mục con và các file cấu hình (.startup, lab.conf). Thư mục mạng ảo đặt tên là BaiTap6



Bước 3: Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

```

GNU nano 6.2 lab.conf
pc1[0]=A
pc2[0]=C
pc3[0]=C
router1[0]=A
router1[1]=B
router2[0]=C
router2[1]=B

```

Bước 4: Trên file PC1.startup, PC2.startup và PC3.startup, thông tin vạch đường được bổ sung vào bảng vạch đường bằng lệnh route add default gw hoặc lệnh route add -net đã giới thiệu

Trả lời:

.file pc1.startup

```
GNU nano 6.2 pc1.startup
ifconfig eth0 195.11.14.5/24 up
route add default gw 195.11.14.1
```

.file pc2.startup

```
GNU nano 6.2 pc2.startup
ifconfig eth0 200.1.1.7/24 up
route add default gw 200.1.1.1
```

.file pc3.startup

```
GNU nano 6.2 pc3.startup
ifconfig eth0 200.1.1.3/24 up
route add default gw 200.1.1.1
```

