

Bài 1. Cài đặt 3 máy tính kết nối với nhau trong mạng. Có thể sử dụng máy ảo (cài VirtualBox) hoặc máy thật. Hệ điều hành sử dụng là Ubuntu. Gọi 3 máy đó là A, B, và C.

Bài 2. Cấu hình mạng cho các máy nằm trong cùng 1 mạng.

(gợi ý: sử dụng lệnh `ifconfig`)

Câu hỏi 1: Trình bày các bước (các lệnh) để thực hiện quá trình cấu hình mạng đó. Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?

Bài 3. Cài đặt wireshark cho máy A. Thử kết nối giữa các máy. Quan sát màn hình wireshark của máy A khi được B và C thực hiện lệnh *ping*.

Câu hỏi 2: Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của lệnh *ping* đó?

Bài 4. Giao thức http: Cài đặt webserver apache2 cho máy A. Thử truy cập vào trang web của A từ 2 máy B và C (cổng 80). Quan sát màn hình wireshark của máy A.

Câu hỏi 3: Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của việc truy cập web đó?

(gợi ý: có thể tham khảo đường link sau để cài đặt apache2: <https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-16-04>)

Câu hỏi 1:

- Trình bày các bước (các lệnh) để thực hiện quá trình cấu hình mạng đó.

Cách 1: sửa file `/etc/network/interface` (đối với ubuntu)

Cách 2: dùng lệnh `ifconfig` để set địa chỉ mạng cho card mạng, cách dùng lệnh như sau: (thực hiện với quyền root)

```
ifconfig <tên card> <IP muốn set> netmask <IP netmask>
```

```
VD: ifconfig eth0 10.0.2.10 netmask 255.255.255.0
```

Sau đó chúng ta gõ lại `ifconfig` để kiểm tra lại

- Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?

Sau khi set IP của 3 máy ảo nằm CÙNG một dải mạng, Chúng ta dùng lệnh `ping` để kiểm tra kết nối giữa các máy, ví dụ: `ping` giữa hai máy 1 và 2 thuộc cùng dải 10.0.2.0/24, nếu `ping` thành công thì là hai máy kết nối thành công, và khi dùng `ifconfig` thấy hai IP cùng một dải mạng thì hai máy đó cùng 1 mạng.

Câu hỏi 2:

Các dòng cho thấy thông tin của lệnh `ping` đó là `echo ping request` và `echo ping reply`, xem ảnh dưới

8	1.375547	192.168.1.6	52.229.169.31	TCP	54	50346 → 443 [ACK] Seq=1 Ack=502 Win=256 Len=0
9	1.563066	192.168.1.6	74.125.200.139	SSL	55	Continuation Data
10	1.617983	74.125.200.139	192.168.1.6	TCP	66	443 → 50690 [ACK] Seq=1 Ack=2 Win=172 Len=0 SLE=1 SRE=2
11	2.332478	192.168.1.6	192.168.1.7	ICMP	74	Echo (ping) request id=0x0001, seq=160/40960, ttl=128 (reply in 12)
12	2.345217	192.168.1.7	192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=160/40960, ttl=128 (request in 11)
13	2.346200	192.168.1.8	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
14	2.599421	192.168.1.6	65.52.108.191	TLSv1	107	Application Data
15	2.645544	192.168.1.8	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	2.844235	65.52.108.191	192.168.1.6	TLSv1	192	Application Data, Application Data

Câu hỏi 3: Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của việc truy cập web đó?

Các dòng có src port là http (80) cổng mặc định của apache

Capturing from Microsoft\NPF_{483C83F4-DCBA-4863-B523-3C4E1B03D06F} [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
222	21:13:58.590670000	10.36.40.181	239.255.255.250	SSDP	528	NOTIFY * HTTP/1.1
223	21:13:58.590877000	fe80::4195:59f3:544ff02::c		SSDP	556	NOTIFY * HTTP/1.1
233	21:13:59.117254000	10.36.40.181	128.119.245.12	HTTP	473	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
241	21:13:59.150482000	128.119.245.12	10.36.40.181	HTTP	452	HTTP/1.1 200 OK (text/html)
242	21:13:59.190558000	10.36.40.181	239.255.255.250	SSDP	556	NOTIFY * HTTP/1.1
243	21:13:59.190758000	fe80::4195:59f3:544ff02::c		SSDP	584	NOTIFY * HTTP/1.1
245	21:13:59.443994000	10.36.40.181	128.119.245.12	HTTP	384	GET /favicon.ico HTTP/1.1
246	21:13:59.462702000	128.119.245.12	10.36.40.181	HTTP	532	HTTP/1.1 404 Not Found (text/html)
247	21:13:59.467414000	10.36.40.181	239.255.255.250	SSDP	542	NOTIFY * HTTP/1.1

Frame 241: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits) on interface 0

Ethernet II, Src: Cisco4c:61:3f (00:1e:f7:4c:61:3f), Dst: HonHaiPr_0a:de:6b (cc:af:78:0a:de:6b)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.36.40.181 (10.36.40.181)

Transmission Control Protocol, Src Port: http (80), Dst Port: 55990 (55990), Seq: 4381, Ack: 420, Len: 398

[5 Reassembled TCP Segments (4778 bytes): #234(1423), #237(1460), #239(1460), #235(37), #241(398)]

HTTP/1.1 200 OK\r\n

Date: Wed, 27 Feb 2013 02:14:00 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n

Last-Modified: Wed, 27 Feb 2013 02:13:01 GMT\r\n

ETag: "d6c97-1194-50408540"\r\n

Accept-Ranges: bytes\r\n

Content-Type: text/html; charset=UTF-8\r\n

Content-Length: 4500\r\n

Connection: Keep-Alive\r\n

Age: 0\r\n

\r\n

0000 cc af 78 0a de 6b 00 1e f7 4c 61 3f 08 00 45 00 ..X..k..La?..E.

0010 01 b6 5f cd 00 00 3a 06 77 18 80 77 f5 0c 0a 24W.w...\$

0020 28 b5 00 50 da b6 70 e7 fd 49 a7 2b b3 a2 50 18 (...P..p..I..+..P

0030 ff ff 16 ab 00 00 70 3e 3c 2f 70 3e 3c 70 3e 54p> </p><p>

0040 68 65 20 65 6e 75 6d 65 72 61 74 69 6f 6a 20 69 the grume ration i

0050 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 73 74 69 n the Co nstitut

0060 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 6a 20 72 op of certain p

Frame (452 bytes) Reassembled TCP (4778 bytes)

Frame (frame), 452 bytes Packets: 336 Displayed: 40 Marked: 0 Profile: Default