NASA HW0 Answer

Part 1

In the class, we have talked about the functionality of the transport layer. One of the protocols that carry out some of these functionalities is called TCP. In this problem, we ask you to find out how to list all the TCP connections (transport layer end-to-end “links”) established on one machine. We will also ask you to list the entries in the routing table, which is used to find out the path to the destination host on the Internet.

Please connect to one of the Linux workstations in our department using SSH. (linux[1-21].csie.ntu.edu.tw) Explain briefly what software you use and how you connect to the workstation.

使用 pietty，連接到 linux1.csie.ntu.edu.tw, port 22, SSH protocol.

Find out what command to use in order to list all on-going TCP connections on this workstation. Please write down the command. (Yes. You are expected to use Google to look for the answer). Copy and paste the relevant part of the response from the command you issued to the workstation, showing the information of all TCP connections.

Command: ‘netstat –a’.

Active Internet connections (servers and established)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|---|---|---|---|---|---|
| tcp | 0 | 0 | *:53158 | *:* | LISTEN |
| tcp | 0 | 0 | *:msnp | *:* | LISTEN |
| tcp | 0 | 0 | localhost:47466 | *:* | LISTEN |

(只列了部分結果)

Pick one of the TCP connections that you get in b) and explain what the value of each field represents.

Example:

tcp 0 0 linux1.csie.ntu.e:46238 charlie.csie.ntu.ed:ssh ESTABLISHED

這是一個 tcp connection，從 linux1.csie.ntu.edu.tw 的 port 46238 連到 charlie.csie.ntu.edu.tw 的 ssh port(22)，狀態為 ESTABLISHED (已建立). Send-Q 和 Recv-Q 都是 0. 兩者分別代表的意義:

Recv-Q: The count of bytes not copied by the user program connected to this socket.

Send-Q: The count of bytes not acknowledged by the remote host.

Execute command ‘route’. This command will show the routing table of the machine. A routing table contains a couple of entries specifying the next host that the packet should be forwarded to when the destination IP address of that packet matches the IP range in a particular routing table entry. Copy and paste the output of the command and briefly explain what each entry in the output routing table is for (and, of course, you probably need to figure out what these fields in the table means: “Destination, Gateway, Genmask, Flags, and Iface”. Google is your friend. ☺)

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---|---|---|---|---|---|---|---|
| default | 140.112.30.254 | 0.0.0.0 | UG | 0 | 0 | 0 | eth0 |
| 140.112.28.0 | * | 255.255.252.0 | U | 0 | 0 | 0 | eth0 |

有兩個 entry
第一個 entry 是 default gateway, 代表沒有 match 任何其他的 entry 的都會實行這個 entry 的內容.Gateway 是 140.112.30.254, 代表要把封包傳給這個 host. Default gateway 的 genmask 是 0.0.0.0 (bit 為 1 的位置才需要比對, 所以表示不用比對), 表示任何 IP 都可以 match. U 代表 route 是正在使用的(up), G 代表是 gateway.
第二個 entry 是 local subnet 使用的, 表示在同一個子網路的機器, 都可以直接往外傳輸(因此 gateway 是*), genmask 則是跟網路設定的子網路遮罩一樣, 這樣才能夠使得在同子網路的機器都可以 match 到這個 entry.
另外, 兩個 entry 的 Iface 都是 eth0, 代表使用這兩個 entry 的封包都要通過 eth0 這張網路卡往外傳輸.

Part 2
假設企業申請了一段 Class C IP，210.74.210.0 (Class C)提供給企業六個部門使用
請問在最大效益的使用率下，該借用幾個 Host ID 用作 Subnet ID？

至少要提供給六個部門使用，$2^3=8 > 6$
3 個 Bits

Subnet Mask 為多少？

255.255.255.224、/27

c) 每個網段最多可提供主機使用的 IP 數量為何？

$2^5-2=30$ 個

Part 3

a) 請於任何可上網的電腦執行 WireShark，抓取 30 秒的紀錄，並使用指令，篩選出 IP “來源 IP 自己，通訊協定為 TCP” 。請寫下指令並將檔案用自己的學號命名 (學號.pcapng)

ip.proto == TCP && ip.dst==本地 IP

(兩種組合可以顛倒)