Network Administration HW0

B04705003 資工三林子雋

1 References

1.1 True/False

1. https://www.lifewire.com/what-is-a-public-ip-address-2625974

2. How many valid NAT mappings can a common NAT support?

3. Is it possible to assign multiple IP addresses to a single device?

4. http://linux.vbird.org/linux_server/0340dhcp.php

5. http://internetofthingsagenda.techtarget.com/definition/gateway

6. What is the exact use of a MAC address?

7. http://dns-learning.twnic.net.tw/dns/03opDNS.html

8. (a) https://www.wikiwand.com/en/Virtual_private_network

   (b) How can I disable IP Security (IPSec) on a VPN connection that uses Layer 2 Tunneling Protocol (L2TP)?

   (c) https://windowsreport.com/vpn-without-encryption/

9. The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords

10. 讀書筆記—TCP Reset 封包的網路攻擊

1.2 Select All that Apply

1. (a) https://www.wikiwand.com/en/Network_layer

   (b) https://www.wikiwand.com/en/Application_layer

   (c) https://www.wikiwand.com/en/IEEE_802.11

2. http://linux.vbird.org/linux_server/0110network_basic/0110network_basic-centos4.php

3. https://www.wikiwand.com/en/Private_network

1.3 Short Answer Questions

1. https://www.linksys.com/us/support-article?articleNum=134478

2. https://www.bestvpn.com/vpns-beginners-need-know/

3. (a) What happens when you type an URL in the browser and press enter?
   (b) https://www.wikiwand.com/en/Transmission_Control_Protocol
   (c) https://www.wikiwand.com/en/Hypertext_Transfer_Protocol

4. https://www.wikiwand.com/en/Peta-

1.4 Basic Command Line Utilities

1. https://stackoverflow.com/questions/3963085/linux-command-to-translate-domainname-to-ip

2. https://www.computerhope.com/unix/utracero.htm

3. (a) http://linux.vbird.org/linux_server/0140networkcommand.php#route
   (b) https://superuser.com/questions/399709/how-to-find-the-gateway-used-for-routing

4. http://linux.vbird.org/linux_server/0140networkcommand.php#route

2 Problem

2.1 True/False

1. False. Because public IP addresses are used to differentiate devices plugged in to the Internet, every public IP address must corresponds to "at most" one device at the same time (there might be some cases that one public ip corresponds to no device).

2. False. There is an upper bound of possible number of NAT mapping, so a single NAT server cannot host an arbitrary number of NAT entries. For example, if an NAT server has only one external public IP address, it will only have maximum 2^{16} possible mappings.

3. False. A device can have multiple interfaces in it. For example, you may have ethernet and WiFi network at the same time, which will result two ip address in the same device.

4. False. The DHCP server has two kinds of policies. One is static IP, the other is dynamic IP. If the DHCP implements dynamic IP policy to the device, it may give different IP to the device each time.

5. False. If the two nodes are in the same LAN, they can send data without passing the gateway.

6. True. If a network interface card receives a packet, it will process this packet if the packet's MAC address match its MAC address.

7. False. The DNS server will query upper layer of other DNS server if it has no record in its database.

8. True. If you send packet without using IPSec, PPTP or other encryption methods, you can send your packets without encryption.

9. False. They all have vulnerabilities which have been proven. Even for the most robust protocol - WPA2, can be broken within 14 hours.

10. True. Because TCP reset attack can force TCP connection to shutdown.

2.2 Select All that Apply

1. Answers is (b), (e). Refer to the explanation below.

   (a) IPv6 is in network layer.

   (b) FTP is in application layer.

   (c) IPsec is in network layer.

   (d) ICMP is in network layer.

   (e) IEEE 802.11ac is in physical layer.

2. Answers are (a), (b), (c). For options (a), (b), (c), their first 20 bits are all "00001100.00100010.0011". The remaining options' first 20 bits are not as same as "00001100.00100010.0011".

3. Answers are (a), (d), (e), because options (b), (c) are out of IPv4 private addresses.

2.3 Short Answer Questions

1. Please refer to Table 1

Table 1: Differences between 2.4G and 5G

	2.4GHz	5GHz
Network Distance Covered Range	Wider Range	Shorter Range
Interference	Higher	Lower
Standard	Using Wireless-B,G, and N	Using Wireless-A, N and AC

2. VPN can:

   (a) Create VPN tunnel(or to say, encrypt your traffic between you and your VPN server).

   (b) Let your ISP unable to know where your connect to, except your connection to the VPN server.

   (c) The IP address which you connect to cannot know your IP address unless the VPN server hands over your details.

3. First, the browser will try to find DNS record in cache (including browser cache, OS cache, router cache and ISP cache). If the browser finds the record, it will translate the domain name into IP address. Otherwise, your ISP will initiate a DNS query to get the IP address of the domain name.

   Second, the browser will initiate a TCP (transport layer protocol, which provide reliable data transfer) connection with the server.

   Third, the browser will follow the HTTP application protocol (a protocol to exchange or transfer hypertext) and send a HTTP request to the web server.

   Fourth, the server handles the request and then sends out HTTP response back to the browser.

   Fifth, after the browser gets the response, the browser can display the content.

4. The computing power is:
$$10^5 \text{ Petaflops} = 10^{20} \text{ flops}$$

   The number of possible combinations of an 128bit key is:

   $$2^{128} \text{ combinations}$$

   The total floating point operation you need to try(worst case):

   $$2^{128} * 1000$$

   how many seconds you need to complete all the operations:

   $$2^{128} * 1000/10^{20} \approx 3.4 * 10^{21} \text{ seconds}$$

   convert seconds to years (assume a year is 365 days):

   $$3.4 * 10^{21}/(365 * 24 * 60 * 60) \approx 1.08 * 10^{14} \text{ years}$$

2.4   Basic Command Line Utilities

1. Execute the following command:

   ```
   $ dig +short <url>
   ```

   Here are the results:

   (a) 140.112.8.116

   (b) 140.112.30.28

   (c) 140.112.30.32

2. Execute the following command:

   ```
   $ traceroute −n google.com
   ```

   Please refer to Figure 1 for the answer.

3. Execute the following command, you will get the routing table.

```
traceroute to google.com (216.58.200.238), 30 hops max, 60 byte packets
 1  10.254.254.254  0.527 ms  1.084 ms  1.332 ms
 2  140.112.149.121  0.464 ms  0.539 ms  0.628 ms
 3  140.112.0.174  0.512 ms  0.583 ms  0.649 ms
 4  140.112.0.190  1.023 ms  1.085 ms  1.338 ms
 5  140.112.0.198  0.958 ms  0.975 ms  0.996 ms
 6  140.112.0.34  14.150 ms  13.983 ms  13.937 ms
 7  72.14.204.212  1.394 ms  1.432 ms  1.493 ms
 8  108.170.244.97  1.765 ms 108.170.244.129  1.889 ms 108.170.244.97  1.751 ms
 9  72.14.237.231  1.545 ms 72.14.238.17  1.522 ms  1.502 ms
10  216.58.200.238  1.832 ms  1.469 ms  1.605 ms
```

Figure 1: Routing path from linux1 workstation to google.com (ip addresses from top to bottom)

```
$ route −n
```

By the routing table (Figure 2), we can get the gateway corresponding to each IP address.

  (a) 140.112.30.254

  (b) 0.0.0.0

  (c) 0.0.0.0 (because linux2.csie.ntu.edu.tw is 140.112.30.33)

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         140.112.30.254  0.0.0.0         UG    0      0        0 net0
10.217.44.0     0.0.0.0         255.255.255.0   U     0      0        0 net1
140.112.30.0    0.0.0.0         255.255.255.0   U     0      0        0 net0
```

Figure 2: Routing table of linux1 workstation

4. Execute the following command.

```
$ ifconfig
```

Please refer to Table 2 for the answers.

Table 2: Internet interfaces and their IPv4 Addresses on linux1

Name	IP Address
lo(loop back, virtual interface)	127.0.0.1
net0	140.112.30.32
net1	10.217.44.32