**True/False**

1.

<http://albert-oma.blogspot.tw/2013/01/nat.html>

False, NAT enables many devices to share one public IP address.

2.

<https://serverfault.com/questions/57878/how-many-valid-nat-mappings-can-a-common-nat-support/57903>

False. Every internal ip:port pair is mapped to an external ip:port pair. An NAT server can only hold its max available port.

3.

<http://linux.vbird.org/linux_server/0110network_basic.php>

True, every device has its own unique IP address, or it will fail to transmit information to the right device. So a device can only have one IP address at the same time.

4.

<http://www.eltoro.com/how-long-does-an-ip-address-stay-attached-to-a-home-or-business/>

False, the IP address assigned by DHCP is dynamic IP address, so it can change.

5.

<https://en.wikipedia.org/wiki/Gateway_(telecommunications)>

False, only if the device connects to the destination outside the LAN will it pass the gateway.

6.

<https://en.wikipedia.org/wiki/MAC_address>

True. Every end device has its unique MAC address and it helps to judge whether itself is the recipient of a packet .

7.

<https://dyn.com/blog/dns-why-its-important-how-it-works/>

False, if the information is not stored locally, computer queries recursive DNS servers. If the recursive servers don’t have the answer, they query the root name servers. It will not immediately fail.

8.

<https://www.google.com.tw/search?ei=uciKWuWYCIu00AS5saDQBA&q=vpn+without+encryption&oq=vpn+with+no+&gs_l=psy-ab.1.5.0l5j0i10k1l3j0.39063.67650.0.73086.26.20.5.1.1.0.167.1554.15j4.19.0....0...1c.1j4.64.psy-ab..1.20.1204...0i67k1j0i7i30k1j0i7i10i30k1j33i160k1j0i10i67k1.0.uU0MJH2UYsY>

True, there are some variants of VPN do not encrypt the traffic or you can simply turn off the encryption function.

9.

[https://en.wikipedia.org/wiki/Wired\_Equivalent\_Privacy#Weak\_security](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy%23Weak_security)

<https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>

False, WEP has many security issues and it is weak and unsafe. WPA is in the intermediate security level. WPA2 is the strongest among the three. So we should choose which to use with concern of security issues.

10.

<https://en.wikipedia.org/wiki/Denial-of-service_attack>

<https://en.wikipedia.org/wiki/TCP_reset_attack>

False, TCP reset attacks is to tamper and terminate the Internet connection by sending forged TCP reset packet. DoS attack seeks to make a machine or network resource unavailable to [users](https://en.wikipedia.org/wiki/User_(computing)) by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems. So the concepts of the two attacks are different.

**Select All that Apply**

1.

<https://en.wikipedia.org/wiki/Network_layer>

<https://en.wikipedia.org/wiki/Data_link_layer>

<https://en.wikipedia.org/wiki/Application_layer>

(b)(e) are not in the Network Layer (b)is in Application Layer; (e)is in Data Link Layer.

2.

<http://linux.vbird.org/linux_server/0110network_basic.php>

Netmask (11111111,11111111,11110000,00000000) -> (255.255.240.0)

(12.34.56.78) AND (255.255.240.0) -> (12.34.48.0)

(a) (12.34.56.123) AND (255.255.240.0) -> (12.34.48.0)

(b) (12.34.63.78) AND (255.255.240.0) -> (12.34.48.0)

(c) (12.34.48.0) AND (255.255.240.0) -> (12.34.48.0)

(d) (12.35.56.78) AND (255.255.240.0) -> (12.35.48.0)

(e) (13.34.56.78) AND (255.255.240.0) -> (13.34.48.0)

(a)(b)(c) are in the same subnet with 12.34.56.78/20.

3.

<https://www.arin.net/knowledge/address_filters.html>

IPv4 private subnet:

**10.0.0.0/8 IP addresses:** 10.0.0.0 -- 10.255.255.255

**172.16.0.0/12 IP addresses:** 172.16.0.0 -- 172.31.255.255

**192.168.0.0/16 IP addresses:** 192.168.0.0 – 192.168.255.255

(a)(d)(e) are valid IPv4 private subnet

**Short Answer Questions**

1.

<https://www.telus.com/en/bc/support/article/dualband-wifi-networks>

(1) 5gHz offers more bandwidth than 2.4gHz.

(2) 5gHz offers less interference than 2.4gHz.

(3) 5gHz covers shorter range, while 2.4gHz covers larger distance.

2.

<https://www.sparklabs.com/viscosity/introtovpn/>

1. Hide your IP address and location.
2. Encrypt your communications.
3. Access your Workplace Remotely

3.

<http://linux.vbird.org/linux_server/0110network_basic.php>

(1). Enter an URL into the address bar.

(2). The browser checks the cache for a DNS record to find IP address.

(3). Browser initiates a TCP connection with the server.

(4). The browser sends request through TCP connection.

(5). The server handles the request and sends back a response.

(6). The server sends out response.

(7). The browser displays the webpage.

4.

the computing power of suuuuuupercomputer is 10^20 flop. The number of flops required per combination check is 1000. So we can do 10^20/10^3 = 10^17 checks per second. It takes 2^128/10^17= 3402823669209384634633.74607431768211456 seconds = 3402823669209384634633.74607431768211456/ (60\*60\*24\*365) = 107902830708060.14188970529154990113 years to brute force an AES-128 key

**Basic Command Line Utilities**

1.

<http://www.pczone.com.tw/vbb3/archive/t-119057.html>

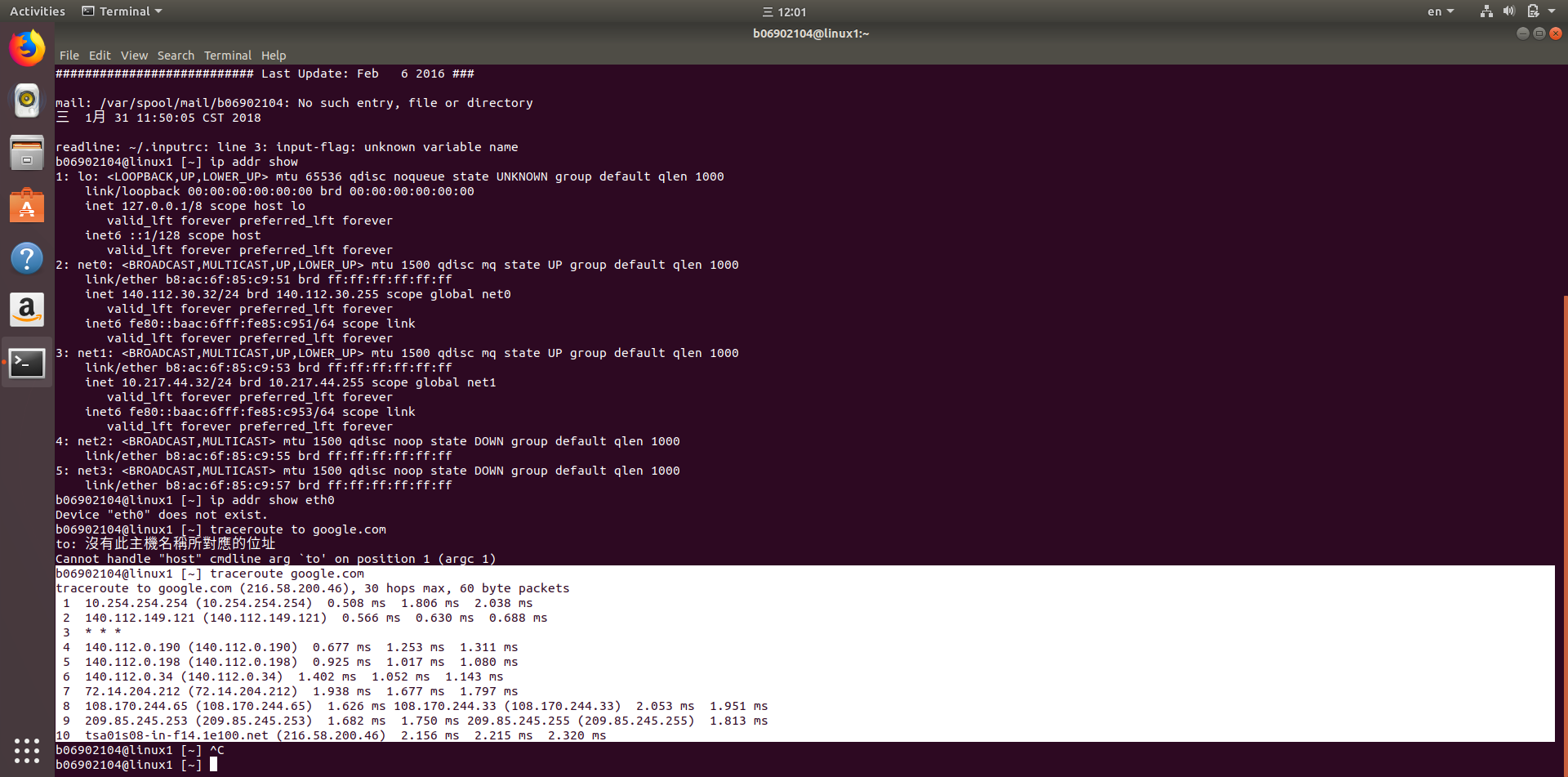
1. ping www.ntu.edu.tw 🡪 140.112.8.116
2. ping csie.ntu.edu.tw 🡪 140.112.30.28
3. ping linux1.csie.ntu.edu.tw 🡪 140.112.30.32

2.

<https://www.wikihow.com/Traceroute>

sign in workstation linux1

traceroute google.com

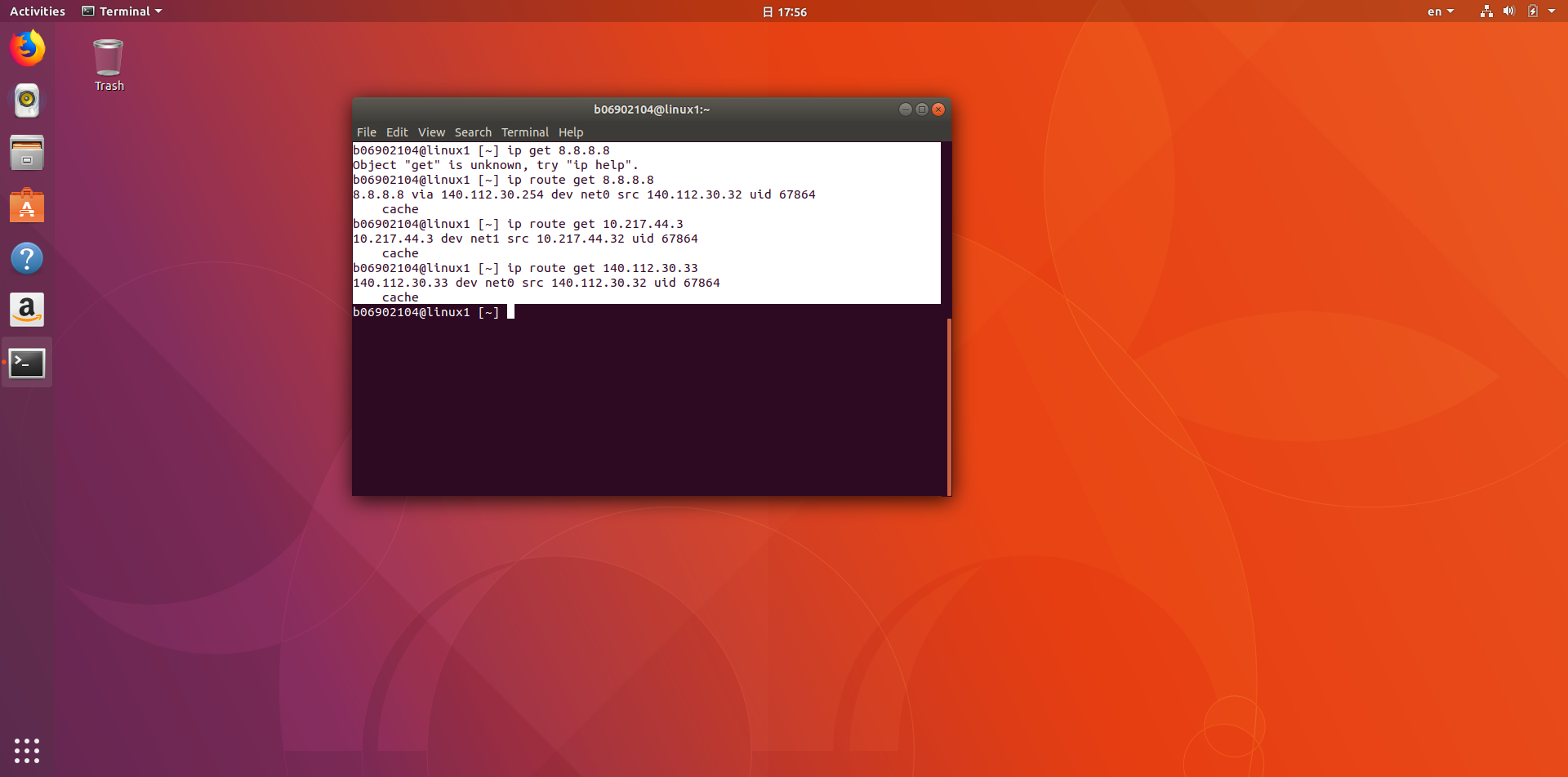


3.

<https://superuser.com/questions/399709/how-to-find-the-gateway-used-for-routing>

1. ip route get 8.8.8.8 -> 140.112.30.254
2. ip route get 10.217.44.3 -> it doesn’t have to pass gateway
3. ping linux2.csie.ntu.edu.tw, to get its IP address -> 140.112.30.33

ip route get 140.112.30.33 -> it doesn’t have to pass gateway



4.

<https://www.cyberciti.biz/faq/linux-list-network-interfaces-names-command/>

/sbin/ifconfig –a

lo : 127.0.0.1; net0 : 140.112.30.32; net1 : 10.217.44.32;

