NASA HW0

B09902004 郭懷元

Network Administration

1. True/False

1. False

> Refernce
>
> https://en.wikipedia.org/wiki/IMT_Advanced
>
> https://en.wikipedia.org/wiki/IMT-2020

Although "4G" and "5G" are more of a marketing term now, *IMT Advanced* and *IMT-2020* are usually the technical standard people refer to when talking about "4G" and "5G". So in *IMT Advanced* and *IMT-2020*, they also have specification for capabilities such as latency, connection density, energy efficiency, etc.

2. False

> Refernce
>
> B09新生手冊

The "5G" in *csie-5G* means 5 GHz, which is the frequency of the WiFi signal.

3. True

> Refernce
>
> 陳可邦 林弘毅
>
> https://www.jannet.hk/zh-Hant/post/network-address-translation-nat/

A NAT server can translate address that includes port.

4. False

> Refernce
>
> 109-1 計算機概論課程內容
>
> https://mkdev.me/en/posts/how-networks-work-what-is-a-switch-router-dns-dhcp-nat-vpn-and-a-dozen-of-other-useful-things

Asscociating multiple devices with one single public IP can be achieved with hiding multiple device under a router. One device (like a laptop or PC) might also have multiple IPs because the device has multiple NIC in it (A PC that has WiFi + Ethernet for example).

5. True

> Refernce
>
> https://medium.com/@zicodeng/how-vpn-works-b7549dcc6ce4
>
> https://networkengineering.stackexchange.com/questions/51159/how-do-vpns-forward-network-traffic-layer-3

A VPN service encrypts and encapsulates the packet sent from your PC, making the packet seems to be sent to the VPN server. The VPN server then decrypts the packet, apply a NAT to the original packet to change its source IP.

6. False

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

A gateway is used to communicate between discrete networks. Since a communication in an intranet might not be a cross-network one, not every packet is necessary to go through the gateway.

7. False

> Reference
>
> https://serverfault.com/questions/373629/what-is-the-correct-response-for-a-dns-server-when-a-domain-does-not-exist

The standard response for non-existent domain is `NXDOMAIN`, and Google Public DNS (`8.8.8.8`) follows the standard.

8. False

> Reference
>
> http://linux.vbird.org/linux_server/0340dhcp.php
>
> https://mkdev.me/en/posts/how-networks-work-what-is-a-switch-router-dns-dhcp-nat-vpn-and-a-dozen-of-other-useful-things

DHCP is used to automaticly set some network parameters, but this progress can be done manually. DNS is used to convert domain names into corresponding IP addresses, but since we already know our destination's IP address, DNS is not needed. NAT is used in routers to convert router's assigned public IP into private IPs of deviced in that LAN, but if both our device and the destination is directly connected to the Internet, NAT isn't necessary.

9. True

> Reference
>
> 陳可邦 林弘毅
>
> https://en.wikipedia.org/wiki/HTTPS
>
> https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

HTTP protocol doesn't encrypt any data.

10. False

> Reference
>
> http://linux.vbird.org/linux_server/0340dhcp.php

DHCP servers only helps managing IPs, the devices will set those parameters themselves, and then the router can communicate directly with the device.

---

2. Short Answer

1.

> Reference
>
> 109-1計算機概論課程內容
>
> https://mkdev.me/en/posts/how-networks-work-what-is-a-switch-router-dns-dhcp-nat-vpn-and-a-dozen-of-other-useful-things
>
> https://en.wikipedia.org/wiki/MAC_address

(a) MAC address

A MAC address a string of number used as a network address. Each network interface controller is assigned with a unique MAC address. This address is used in layer 2 of OSI model. Ethernet, WiFi, and Bluetooth all use MAC addresses.

(b) Router

Routers can connect different LANs, route packets from one network to another network. They work on layer 3 of OSI model, and use IP address to direct packets.

(c) Switch

Switches work on layer 2 of OSI model. They use MAC address to direct frames from one device to another, and they connect hosts to form a LAN.

2.

> Reference
>
> https://www.jannet.hk/zh-Hant/post/IP-Address-Version-4-IPv4
>
> https://www.netadmin.com.tw/netadmin/zh-tw/technology/D5162EE38674405EADB022E0802A05B2
>
> https://www.twbsd.org/cht/book/ch05.htm

A subnet mask is a string of number that can be used to identify the network prefix of an IP address. When the subnet mask of an IP address is applied by a bitwise AND to the IP address, the IP address's network prefix is yielded. If two valid IP address have the same network prefix when applied with the same mask, they are in the same subnet.

From `192.168.0.1/23`, we know:

	Binary form	**Dot-deciml form**
IP address	`11000000.10101000.00000000.00000001`	`192.168.0.1`
Subnet mask	`11111111.11111111.11111110.00000000`	`255.255.254.0`
Network prefix	`11000000.10101000.00000000.00000000`	`192.168.0.0`

(a) `192.167.0.1` No

Its network prefix is `192.167.0.0`, which is different, therefore is not in the same subnet.

(b) `192.168.0.0` Yes

It has the same network prefix, and is a valid IP address. But this address is the network address of this subnet, therefore cannot be assigned to a host.

(c) `192.168.1.0` Yes

It has the same network prefix, and is a valid IP address too.

(d) `193.168.0.1` No

Its network prefix is `193.168.0.0`, which is different, therefore is not in the same subnet.

3.

(a) DoS

> Reference
>
> https://ithelp.ithome.com.tw/articles/10188774
>
> https://en.wikipedia.org/wiki/Denial-of-service_attack

A DoS (denial-of-service) attack's goal is to keep other users from using this service. This can be done by using different attack techniques (such as flooding the target with packets) to exhaust the target service/machine's resource or bandwith. Defense to this kind of attack aims to block malicious traffic and allow legitimate traffics, and can be achieved with combination of attack detection and traffic classification.

(b) DDoS

> Reference
>
> https://ithelp.ithome.com.tw/articles/10188774
>
> https://en.wikipedia.org/wiki/Denial-of-service_attack

A DDoS (distributed DoS) attack is essentially a DoS attack that uses multiple unique IP address or machine. An attacker can gain control of thousands of systems infected with malware or virus, then use them to send a DDoS attack. The principles of defense are the same as a DoS attack, but difficulty of defense against a DDoS attack might be harder, since there are more malicious machines.

(c) Man-in-the-middle attack

> Reference
>
> https://en.wikipedia.org/wiki/Man-in-the-middle_attack

A man-in-the-middle (MITM) attack is when two parties wants to communicate, the attacker becomes part of the communication path, and the attacker secretly intercepts then relays and change the message. This attack can be done by various techniques, such as DNS spoofing, IP spoofing. One defense against this attack is authentication. A trusted third party can provide certification of the ownership of a public key, thus ensure the process of key exchange.

4.

> Reference
>
> https://en.wikipedia.org/wiki/Internet_protocol_suite
>
> https://en.wikipedia.org/wiki/Physical_layer
>
> http://securityalley.blogspot.com/2014/06/data-link-layer.html
>
> https://en.wikipedia.org/wiki/Internet_layer

The five layer of **five-layer internet protocol stack** are:

- Physical layer
    - Means of transmitting raw bits is defined in this layer. Protocols in this layer might have specification for things like radio frequencies, design of cables, or pin definitions.
    - Service example: Standardized physical interface like USB.
- Data link layer
    - This layer is where hardware and software meet. Most of the services provides by this layer is implemented in network interface. MAC addresses are used in this layer to direct traffics.
    - Service example: Packing network layer data packets into frames.
- Internet layer
    - This layer is in responsible for tranfering packets across networks.
    - Service example: Routing.
- Transport layer
    - This layer establishes reliable, end-to-end channel for applications to communicate with each other.
    - Service example: Flow control.
- Application layer

  - This layer contains protocols that are directly used by applications to standardize communications.
  - Service example: Text transfer.

5.

> Reference
>
> https://ithelp.ithome.com.tw/articles/10205476
>
> https://en.wikipedia.org/wiki/User_Datagram_Protocol
>
> https://en.wikipedia.org/wiki/Transmission_Control_Protocol

UDP

UDP is a protocol in tranport layer that uses a minimum if mechanism to establish a communication channel between applications. It's also a connectionless protocol. Datas transmitted through UDP aren't guaranteed to be recieved by the destination, and the order of packets isn't guaranteed too. UDP only provides a checksum for integrity check.

TCP

TCP on the other hand provides a reliable transmission and is connection-oriented. There are three main parts of TCP's operation, *connection establishment*, *data transfer*, and *connnection termination*. Communications under TCP are two-way, therefore reliabiliy can be unsured. Order of packets are ensure in TCP.

Pros & Cons

UDP has fewer packets needed to be sent (one way communication) and smaller packet size compared to TCP, and UDP also consumes less resources. TCP however has the reliability that UDP lacks.

Application

UDP can be used in video streaming, since occasional frame drops don't affect user experience too much. TCP can be used in cloud drive file transfering, because cloud drives are meant to keep all the content of uploaded files, we have to ensure all packets arrive and are in order.

---

3. Command Line Utilities

1.

> Refernce
>
> https://www.cloudns.net/blog/10-most-used-nslookup-commands/
>
> https://ithelp.ithome.com.tw/articles/10214407

(a) `www.ntu.edu.tw` : `140.112.8.116`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [16:55:44]
$ nslookup www.ntu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.ntu.edu.tw
Address: 140.112.8.116
```

(b) `csie.ntu.edu.tw` : `140.112.30.26`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [16:55:52]
$ nslookup csie.ntu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   csie.ntu.edu.tw
Address: 140.112.30.26
```

(c) `linux1.csie.ntu.edu.tw` : `140.112.30.32`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [16:56:00]
$ nslookup linux1.csie.ntu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   linux1.csie.ntu.edu.tw
Address: 140.112.30.32
```

(d) `ceiba.ntu.edu.tw` : `140.112.161.178`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [16:56:06]
$ nslookup ceiba.ntu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ceiba.ntu.edu.tw
Address: 140.112.161.178
```

2.

(a)

> Reference
>
> https://opensource.com/article/18/5/how-find-ip-address-linux

Public IP: `140.112.150.127`, Private IP: `192.168.50.52`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [17:04:26]
$ hostname -I | awk '{print $1}'
192.168.50.52
(base)
# frank @ Frank-Desktop-Linux in ~ [17:08:35]
$ curl ifconfig.me
140.112.150.127
```

(b)

> Refernce
>
> https://www.cloudns.net/blog/10-most-used-nslookup-commands/
>
> https://ithelp.ithome.com.tw/articles/10214407

DNS server IP: `140.112.254.4`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [17:24:28]
$ nslookup csie.ntu.edu.tw
Server:         140.112.254.4
Address:        140.112.254.4#53

Non-authoritative answer:
Name:   csie.ntu.edu.tw
Address: 140.112.30.26
```

Delegation path:

`b.root-servers.net` ⇒ `g.dns.tw` ⇒ `moemoon.edu.tw` ⇒ `dns.tp1rc.edu.tw` ⇒ `csman.csie.ntu.edu.tw`

```
(base)
# frank @ Frank-UX425EA-Linux in ~ [14:20:08]
$ dig +trace csie.ntu.edu.tw | grep Received
;; Received 1137 bytes from 140.112.254.4#53(140.112.254.4) in 3 ms
;; Received 1004 bytes from 199.9.14.201#53(b.root-servers.net) in 223 ms
;; Received 784 bytes from 220.229.225.195#53(g.dns.tw) in 7 ms
;; Received 382 bytes from 192.83.166.17#53(moemoon.edu.tw) in 3 ms
;; Received 117 bytes from 163.28.16.10#53(dns.tp1rc.edu.tw) in 3 ms
;; Received 1365 bytes from 140.112.30.13#53(csman.csie.ntu.edu.tw) in 0 ms
```

(c)

> Reference
>
> https://unix.stackexchange.com/questions/612416/why-does-etc-resolv-conf-point-at-127-0-0-53
>
> https://security.stackexchange.com/questions/13900/if-i-use-a-vpn-who-will-resolve-my-dns-requests

DNS server IP: `127.0.0.53` / `192.168.50.1`

```
(base)
# frank @ Frank-Desktop-Linux in ~ [16:55:52]
$ nslookup csie.ntu.edu.tw
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   csie.ntu.edu.tw
Address: 140.112.30.26
```

```
C:\Users\frank>nslookup
預設伺服器:  router.asus.com
Address:  192.168.50.1
>
```

Because the Ubuntu version I'm running uses `systemd-resolve` to handle DNS queries and the network setting of my PC is configured by DHCP, `systemd-resolve` shows a symbolic link to `127.0.0.53`(a loopback address). `systemd-resolve` itself forwards DNS queries to the 'real' DNS server ip, which can be found in Windows quite easily.

When using this specific VPN service, the DNS server we use is reassigned and is configured at the VPN host server, instead of the DNS server we originally set. Therefore, we have different DNS server IP.

(d)

> Reference
>
> https://www.cyberciti.biz/faq/traceroute-tracepath-unix-linux-command/

Route path: my PC ⇒ router (which is also a DNS server) at home (at `192.168.50.1`)

```
(base)
# frank @ Frank-Desktop-Linux in ~ [23:52:03]
$ traceroute 192.168.50.1
traceroute to 192.168.50.1 (192.168.50.1), 30 hops max, 60 byte packets
 1  router.asus.com (192.168.50.1)  0.317 ms  0.297 ms  0.368 ms
```

System Administration

1. Capture The Flag

1.

Flag: `NASA{echo_$USER}`, `NASA{id_-u_-n}`, `NASA{whoami}`

> Reference
>
> 陳可邦 林弘毅
>
> https://www.cyberciti.biz/faq/appleosx-bsd-shell-script-get-current-user/

2.

Flag: `NASA{ssh_bbsu@ptt.cc}`

> Refernce
>
> https://chakra-zh.blogspot.com/2013/02/chakra-linux-ssh-ptt.html

3.

Flag: `NASA{man_man}`

> Reference
>
> B09前瞻營課程內容&手冊

4.

Flag: `NASA{71_921}`

> Reference
>
> https://cmdlinetips.com/2011/08/how-to-count-the-number-of-lines-words-and-characters-in-a-text-file-from-terminal/

```
cd ~
ls -lah
chmod 777 toilet
cd toilet
wc -l article
wc -w article
```

5.

Flag: `NASA{MEOW_CAT}`

> Reference
>
> B09前瞻營課程內容&手冊
>
> https://stackoverflow.com/questions/18006581/how-to-append-contents-of-multiple-files-into-one-file

```
cd ~/carton
ls -lah
cat *
cat flag0* flag1* flag2*
cat flag2* flag3* flag4* flag5*
```

or

```
cd ~/carton
ls -lah
cat * | more
```

6.

Flag: `NASA{IM_SHERLOCKED}`

> Reference
>
> B09前瞻營課程內容&手冊

```
cd ~/TW
mkdir CSIE
chmod 700 CSIE
mv hide CSIE
cd CSIE
mkdir vote
chmod 700 vote
mv hide vote
cd vote
mkdir box
chmod 700 box
mv hide box
cd box
./hide
```

7.

Flag: `NASA{grep_virus_nasa}`

> Refernce
>
> http://benjr.tw/97395
>
> https://www.cyberciti.biz/faq/grep-regular-expressions/

```
cd ~
grep -E "NASA\{[[:alpha:]]+_virus_[[:alpha:]]+\}" flags
```

or

```
cd ~
cat flags | grep -E "[[:alpha:]]+_virus_" | grep -E "_virus_[[:alpha:]]+"
```

8.

Flag: `NASA{12402_0_1000000}`

> Reference
>
> B09前瞻營課程內容&手冊
>
> http://linux.vbird.org/linux_basic/0330regularex.php#sed_file

```
cd ~/nanasasa
cp nasa_report clone
sed -i 's/nasa/NASA/g' clone
./test clone
```

9.

Flag: `NASA{UR_MAZ3_RUNN3R}`

> Reference
>
> https://blog.gtwang.org/linux/unix-linux-find-command-examples/
>
> https://stackoverflow.com/questions/3458461/find-file-then-cd-to-that-directory-in-linux

```
cd ~/maze
find -name flag
cat $(find -name flag)
```

10.

Flag: `NASA{0BS3RV3_M3}`

> Reference
>
> 陳可邦 林弘毅
>
> https://www.twblogs.net/a/5b7afe162b7177539c2499ab
>
> https://linuxize.com/post/vim-search/
>
> https://blog.gtwang.org/useful-tools/how-to-use-vim-as-a-hex-editor/

In bash:

```
cd ~/image
cat url
wget $(cat url) -O pic.jpg
vim pic.jpg
```

In vim:

```
:%! xxd
/NA
/SA
```

or without vim

```
cd ~/image
cat url
wget $(cat url) -O pic.jpg
strings pic.jpg | grep NASA
```

11.

Flag: `NASA{kill_-9_$(pgrep_guineaPig)}`, `NASA{pkill_-9_guineaPig}`

> Reference
>
> 陳可邦 林弘毅
>
> B09前瞻營課程內容&手冊
>
> https://blog.gtwang.org/linux/linux-howto-find-process-by-name/

After running `guineaPig`, first press `ctrl`+`z` to stop the process. Then apply the command to kill the process.

12.

> Reference
>
> https://david50.pixnet.net/blog/post/45252072-%5B%E7%AD%86%E8%A8%98%5Dlinux---top%E8%B3%87%E8%A8%8A
>
> https://stackoverflow.com/questions/17394356/how-can-i-make-a-bash-command-run-periodically
>
> http://linux.vbird.org/linux_basic/0430cron.php

First, I use `top -o S` to see what processes are running, and I find out that the process that is printing the message is not constantly running (because the number of running processes is 1 most of the time). Then, I use `crontab -l` to see if there are any scheduled jobs, and find the command is there (it's also the only one in the table). Finally, I use `crontab -r` to remove all the scheduled jobs. Problem solved!

13.

> Reference
>
> https://unix.stackexchange.com/questions/6050/is-it-possible-to-stop-a-shutdown-command
>
> https://stackoverflow.com/questions/5050780/detect-pending-linux-shutdown
>
> https://unix.stackexchange.com/questions/56083/how-to-write-a-shell-script-that-gets-executed-on-login

Since it's a auto shutdown, it's probably a script that runs at login or startup and schedules a shutdown. First, I run `cat /run/systemd/shutdown/scheduled` to see if any shutdowns are scheduled, and there is one. Then I run `shutdown -c` to cancel it to fix the problem for now.

Now, I want to find where the script or command is at. I check `~/.profile`, `/etc/profile`, files under `/etc/profile.d` but nothing strange was there. Then I run `bash` and run `cat /run/systemd/shutdown/scheduled` in the newly started bash. A scheduled shutdown appears, so that means the command is in `~/.bashrc`. Finally run `vim ~/.bashrc`, `/shutdown`, remove the line, save and exit.

14.

> Reference
>
> B09前瞻營課程內容&手冊
>
> https://wiki.archlinux.org/index.php/File_permissions_and_attributes

The `r`, `w`, and `x` mean different permissions as the table below.

Permissions	Meaning to a file	Meaning to a directory
`r`	Permission to read the file	Permission to show content of the directory
`w`	Permission to modify the file	Permission to modify content of the directory (such as renaming files or folders, creating new files or folders)
`x`	Permission to execute the file	Permission to access the directory with `cd`

15.

> Reference
>
> https://www.geeksforgeeks.org/linux-file-hierarchy-structure/
>
> https://man.archlinux.org/man/file-hierarchy.7

`/bin`

Contains binary executables of commands essential in single user mode, and for all users.

`/dev`

Contains device files of any device attached to the system. A device file is an interface where a device driver can interact with the device.

`/etc`

Contains configuration files that are system-wide.

`/tmp`

Where small temporarily files go. This directory is flushed at bootup, and files in it that haven't been accessed for a certain time will be automatically removed.

`/usr`

Contains binaries, libraries, documents, source codes and other files of second level applications. This directory should be read-only and sharable.