

Linux Basic

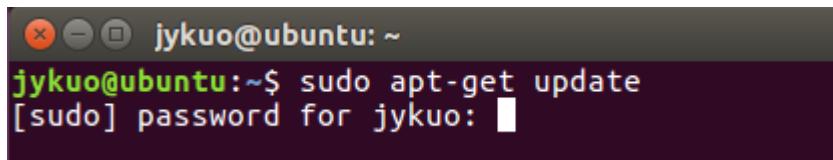
郭忠義

jykuo@ntut.edu.tw

臺北科技大學資訊工程系

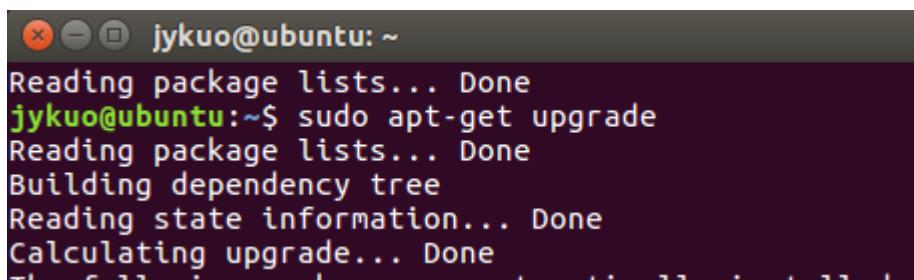
SSH連線

- 安裝完Ubuntu，更新、升級安裝程式
 - lsb_release -a，查看 Ubuntu版本
 - unmae -a，cat /proc/version，查看核心版本
 - sudo apt-get update



```
jykuo@ubuntu:~$ sudo apt-get update  
[sudo] password for jykuo: [REDACTED]
```

- sudo apt-get upgrade，之後按Y(需要十幾分鐘)



```
jykuo@ubuntu:~$ sudo apt-get upgrade  
Reading package lists... Done  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Calculating upgrade... Done  
The following packages will be upgraded: 100 packages
```

SSH連線

□ Linux安裝SSH，sudo apt-get install ssh

- 若有出現此錯誤訊息

```
kernel@ubuntu:~$ sudo apt-get install ssh
[sudo] password for kernel:
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is an
other process using it?
kernel@ubuntu:~$
```

- 刪除 apt程序，sudo kill -9 apt
- 刪除 lock 檔案
 - sudo rm /var/lib/dpkg/lock
 - sudo rm /var/lib/apt/lists/lock
 - sudo rm /var/cache/apt/archives/lock
- 更新套件
 - sudo dpkg --configure -a
 - sudo apt-get update

```
kernel@ubuntu:~$ sudo kill -9 apt
[sudo] password for kernel:
kill: failed to parse argument: 'apt'
kernel@ubuntu:~$ sudo rm /var/lib/dpkg/lock
kernel@ubuntu:~$ sudo rm /var/lib/apt/lists/lock
kernel@ubuntu:~$ sudo rm /var/cache/apt/archives/lock
kernel@ubuntu:~$ sudo dpkg --configure -a
dpkg: error: need an action option

Type dpkg --help for help about installing and deinstalling packages.
Use 'apt' or 'aptitude' for user-friendly package management.
Type dpkg -Dhelp for a list of dpkg debug flag values;
Type dpkg --force-help for a list of forcing options;
Type dpkg-deb --help for help about manipulating *.deb files.

Options marked [*] produce a lot of output - pipe it to less
kernel@ubuntu:~$ sudo apt-get update
```

SSH連線

□ 查詢虛擬機IP

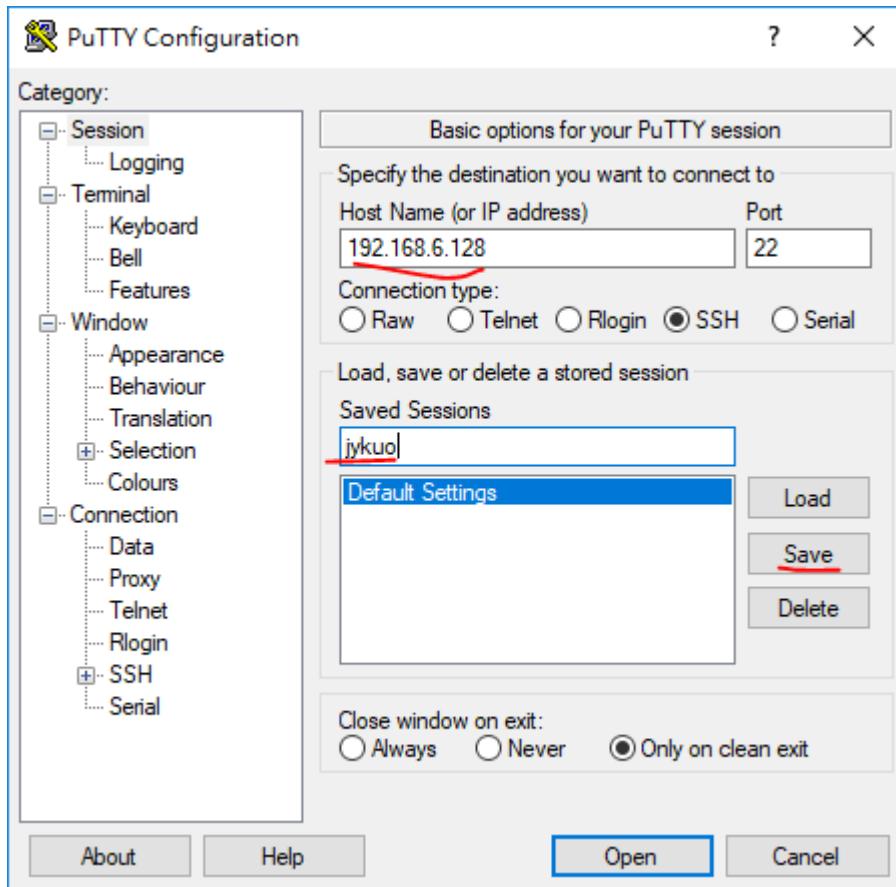
○ ifconfig

```
jykuo@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:ae:d7:fa
            inet addr:192.168.6.128 Bcast:192.168.6.255 Mask:255.255.255.0
            inet6 addr: fe80::79b9:602:4172:77fc/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:267506 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:122151 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:401850759 (401.8 MB) TX bytes:7439750 (7.4 MB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:65536 Metric:1
                  RX packets:314 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:27510 (27.5 KB) TX bytes:27510 (27.5 KB)
```

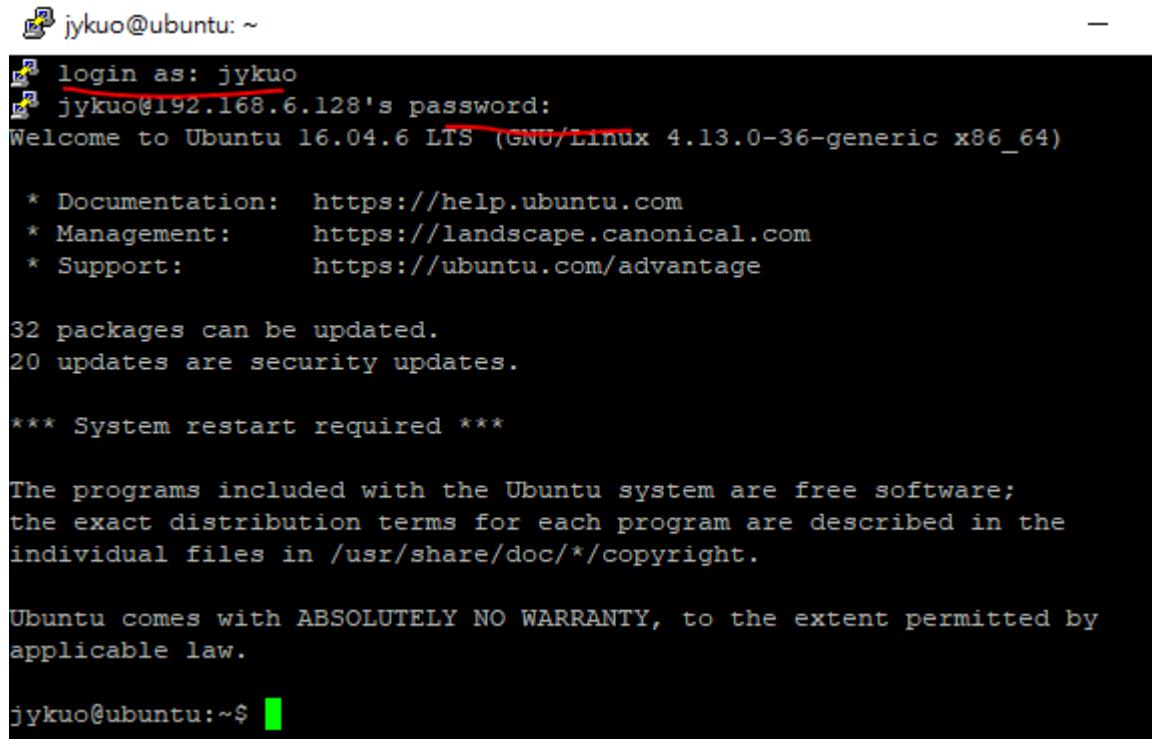
SSH連線

- 本機端(Host OS)，下載PuTTY，安裝、執行
 - 輸入虛擬機ip，預設port 22，儲存設定



SSH連線

□ 使用PuTTY登入虛擬機 Terminal



jykuo@ubuntu: ~

```
login as: jykuo
jykuo@192.168.6.128's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.13.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

32 packages can be updated.
20 updates are security updates.

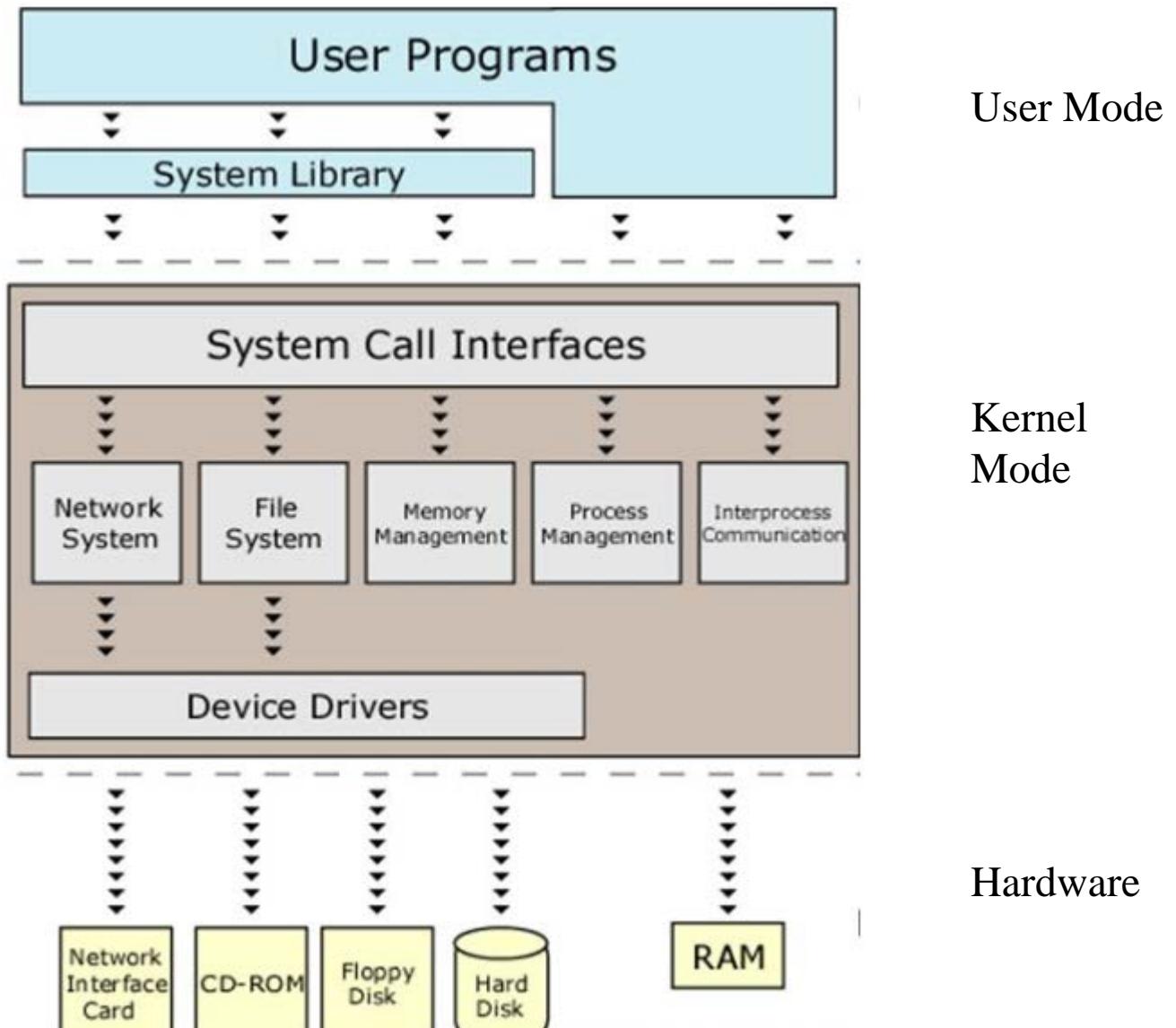
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jykuo@ubuntu:~$
```

Linux 核心架構



User Mode

Kernel
Mode

Hardware

Linux 系統目錄

□ 系統目錄內容

- /：根目錄，包含整個Linux系統的所有目錄和檔案。
- /bin：放置操作系統所需各種指令程式。如cp、rpm、kill、tar、mv、rm與ping等，及各種不同shell，如bash、zsh、tcsh等。
- /boot：系統啟動時須讀取的檔案，包括系統核心。
- /dev：存放周邊設備代號的檔案。例如硬碟/dev/sda、終端機/dev/tty0等。它們實際上都指向所代表的周邊設備。
- /etc：與系統設定、管理相關檔案。例如記錄帳號名稱的passwd檔、投影密碼檔shadow。
- /etc/rc.d：包含開機或關機時所執行的script檔案。
- /home：使用者帳號的家目錄。
- /lib：共用的函式庫。
- /lib/modules：存放系統核心模組。某些可模組化部份，不需在編譯系統核心時放入核心，避免核心過大導致效率低落。

Linux 系統目錄

- /lost+found：檔案系統發生問題，Linux自動掃描磁碟修正錯誤，若找到遺失或錯誤區段，會轉成檔案存放於此，等管理員處理。
- /media：做為光碟、軟碟、隨身碟與其他分割區自動掛載點。
- /mnt：手動掛載其他分割區的掛載點。
- /proc：系統核心和執行程序間的資訊，執行ps、free等指令時看到訊息從這裡讀取。目錄內檔案是虛擬檔案。
- /root：系統管理者專用目錄，root帳號的家目錄。
- /sbin：啟動系統需執行的程式，如fsck、init與swapon等。
- /tmp：使用者暫時放置檔案的目錄。系統預設讓所有使用者讀取、寫入和執行。某些程式執行中產生臨時檔也存放在此。
- /usr：存放系統指令、程式等資訊。

Linux 系統目錄

- /usr/bin：使用者可執行的指令程式，如find、free、gcc等。
- /usr/local：自行編譯的軟體，以便與使用RPM安裝的軟體區隔，避免兩個套件系統發生衝突。
- /usr/share/doc：存放各種文件的目錄。
- /usr/share/man：放置多種線上說明文件。
- /usr/src：存放原始碼、Linux系統核心原始碼等。
- /var：放系統執行時，內容經常變動的資料或暫存檔。包括使用者郵件、記載系統活動過程log檔、列印工作佇列檔、系統執行程式的PID(ProcessID，程序識別碼)記錄等。Apache網頁目錄與FTP目錄等伺服器的專用目錄也位於此。
- /var/tmp：管理者通常定時清理/tmp目錄維護磁碟空間。若不想將檔案放入/tmp，避免遭管理者刪除，可存放在此。

基本指令-壓縮

□ compress

- 壓縮及解壓縮檔名為 .Z 的壓縮檔。
- compress 壓縮會將原檔案刪除變成檔名為 .Z 的檔案。
- 解壓縮，壓縮檔不見，只剩下被解壓縮的檔案
- compress XXXXX <== 將 XXXXX 檔案壓縮成為 XXXXX.Z 檔名
- compress -d XXXXX.Z <== 將 XXXXX.Z 解壓縮成 XXXXX
- 解壓縮也可用 uncompress XXXXX.Z 來達成！

基本指令-壓縮

□ gzip

- 壓縮檔名為 .gz
- gzip XXXXX <==這是壓縮指令
- gzip -d XXXXX.gz <==這是解壓縮指令

□ tar

- tar -cvf bird.tar bird <==只將目錄轉成一個檔案，沒有壓縮
- tar -zcvf bird.tar.gz bird <==壓縮一整個目錄成為 .tar.gz 檔案
- 解壓縮
 - tar -xvf bird.tar
 - tar -zxvf bird.tar.gz
- tar 壓縮及解壓縮，原檔案與產生檔案同時存在

基本指令-網路資訊

□ hostname

- 觀看主機名稱。

```
jykuo@ubuntu:~$ hostname  
ubuntu  
jykuo@ubuntu:~$ █
```

□ ping

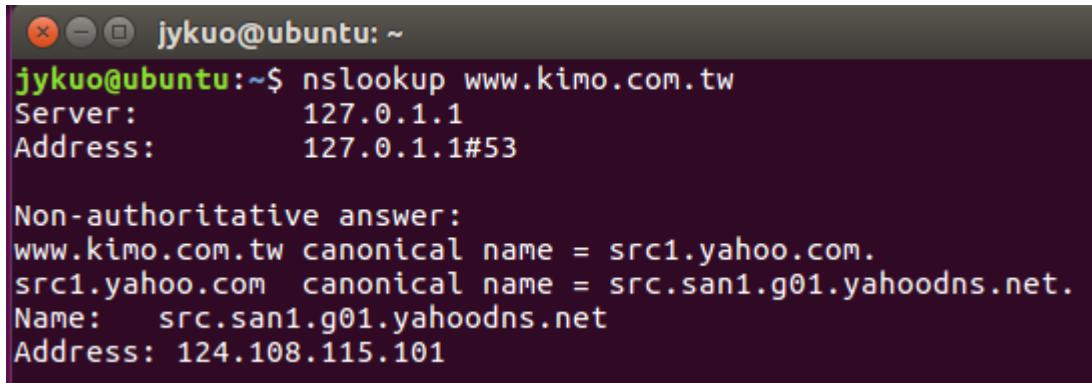
- 查看對方網路是否有動作的指令
- ping 是兩部主機之間的回聲與否判斷

```
Ubuntu: ~  
jykuo@ubuntu:~$ ping www.ntut.edu.tw  
PING www.ntut.edu.tw (140.124.13.105) 56(84) bytes of data.  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=1 ttl=128 time=1.55 ms  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=2 ttl=128 time=2.42 ms  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=3 ttl=128 time=2.33 ms  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=4 ttl=128 time=2.28 ms  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=5 ttl=128 time=2.50 ms  
64 bytes from ctll.ntut.edu.tw (140.124.13.105): icmp_seq=6 ttl=128 time=3.05 ms
```

基本指令-網路資訊

□ nslookup

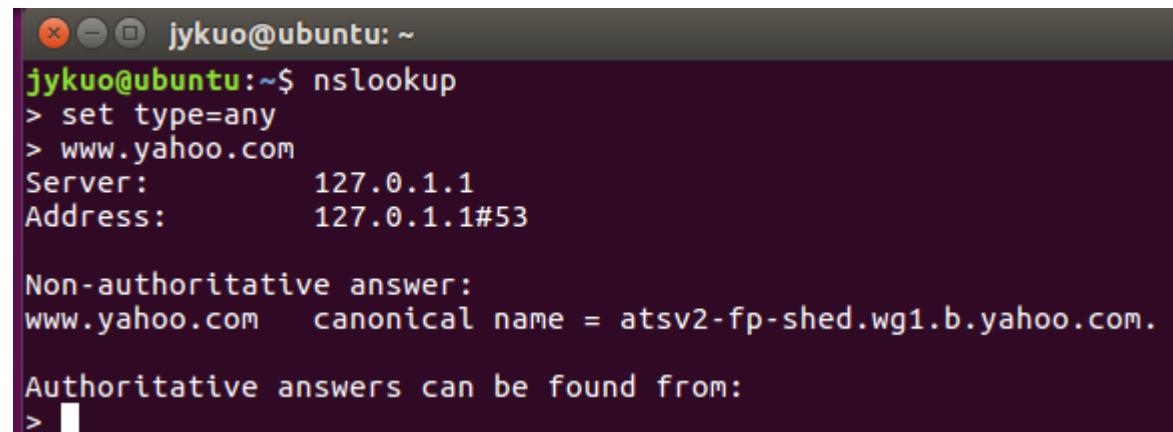
- 查詢或反查詢 DNS 指令，
- 例如要知道奇摩網路位址：nslookup www.kimo.com.tw



```
jykuo@ubuntu:~$ nslookup www.kimo.com.tw
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
www.kimo.com.tw canonical name = src1.yahoo.com.
src1.yahoo.com canonical name = src.san1.g01.yahoodns.net.
Name:    src.san1.g01.yahoodns.net
Address: 124.108.115.101
```

- 詳細查詢



```
jykuo@ubuntu:~$ nslookup
> set type=any
> www.yahoo.com
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
www.yahoo.com canonical name = atsv2-fp-shed.wg1.b.yahoo.com.

Authoritative answers can be found from:
>
```

基本指令-網路資訊

□ traceroute

- sudo apt-get install traceroute
- traceroute www.ntut.edu.tw
- 追蹤兩部主機間通過的各個節點通訊狀況。例如連線到 yahoo 的速度比平常慢，可能 (1) 網路環境有問題，(2) 外部 Internet 有問題。
- 連接目的地所有 router 進行 ICMP回聲等待，例如由連接到 Yahoo ，會經過幾個節點，對這些節點做 ICMP 回聲等待，偵測回覆時間，每個節點會偵測三次。解析後可瞭解這條連線是那個環節出問題。
- 如果預設 5 秒內聽不到節點的回聲，螢幕會顯示 * ，告知該節點無法有順利的回應。由於traceroute 用 ICMP ，有些防火牆或主機會封鎖，有些 gateway 不支援 traceroute 。

基本指令-網路資訊

□ ip link show

```
jykuo@ubuntu:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEF
up default qlen 1000
    link/ether 00:0c:29:ae:d7:fa brd ff:ff:ff:ff:ff:ff
```

□ ip -s link show

```
jykuo@ubuntu:~$ ip -s link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT gro
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX: bytes   packets   errors   dropped overrun mcast
        21210      246       0       0       0       0
    TX: bytes   packets   errors   dropped carrier collsns
        21210      246       0       0       0       0
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode UP
up default qlen 1000
    link/ether 00:0c:29:ae:d7:fa brd ff:ff:ff:ff:ff:ff
    RX: bytes   packets   errors   dropped overrun mcast
        8847005    9847       0       0       0       0
    TX: bytes   packets   errors   dropped carrier collsns
        284287    3612       0       0       0       0
```

基本指令-網路資訊

□ route

- 用來看網路通訊包傳送的路由情況。由於通信包是藉由一個個路由表傳遞，所以觀察路由表，對網路除錯很重要

基本指令-網路資訊

□ netstat -an

- 觀察網路狀況。
- 查看某個網路服務是否啟動，查詢網路介面監聽的埠口 (port) 是否真有啟動。

```
Terminal File Edit View Search Terminal Help
jykuo@ubuntu:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 127.0.1.1:53              0.0.0.0:*
tcp      0      0 0.0.0.0:22              0.0.0.0:*
tcp      0      0 127.0.0.1:631             0.0.0.0:*
tcp6     0      0 :::22                   :::*
tcp6     0      0 ::1:631                 :::*
udp      0      0 0.0.0.0:5353             0.0.0.0:*
udp      0      0 127.0.1.1:53             0.0.0.0:*
udp      0      0 0.0.0.0:68               0.0.0.0:*
udp      0      0 0.0.0.0:57853            0.0.0.0:*
udp      0      0 0.0.0.0:631              0.0.0.0:*
udp      0      0 0.0.0.0:60495            0.0.0.0:*
udp6     0      0 :::5353                 :::*
udp6     0      0 ::::58955              :::*
raw6     0      0 ::::58                 :::*
7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State         I-Node    Path
unix    2      [ ACC ]     STREAM   LISTENING    19644    /run/systemd/private
unix    2      [ ACC ]     STREAM   LISTENING    30993    @/tmp/.ICE-unix/1698
unix    2      [ ACC ]     DGRAM
18
```

基本指令-網路連線

□ /etc/hosts.allow 允許連線

- ldd (list dynamic dependencies, 列出動態函式庫依賴關係)
 - hosts.allow 屬於tcp_Wrappers防火牆的配置文件，ssh需要應用 libwrapped函式庫
 - ldd /usr/sbin/sshd |grep libwrap.so.0，測試sshd是否使用該函式庫

```
kjy@node01:~$ ldd /usr/sbin/sshd |grep libwrap
    libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007f02bb524000)
```

○ sudo gedit /etc/hosts.allow

- 如新增sshd:192.168.6.，允許192.168.6網段IP與系統進行ssh連線。

```
kjy@node01:~$ more /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                         See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#                  ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd:192.168.6.
```

基本指令-網路連線

□ /etc/hosts.allow 允許連線

○ 另一台虛擬機連線

```
kjy@ubuntu:~$ ssh 192.168.6.135
The authenticity of host '192.168.6.135 (192.168.6.135)' can't be established.
ECDSA key fingerprint is SHA256:1EQvXCIuKXo9TWMocWQmmWOHjepOA0mfgruMaulBZZ0.
Are you sure you want to continue connecting (yes/no)? yes
```

基本指令-網路連線

□ 拒絕連線。

- sudo gedit /etc/hosts.deny

- 例如新增sshd:all代表不允許任何IP與系統進行ssh連線。

- 當兩者設定有衝突時，系統將以hosts.allow為主。

sshd: ALL

```
kjy@node01:~$ more /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                                     See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#                  ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
sshd:ALL
```

基本指令-網路連線

- 關閉root身分ssh連線。
 - sudo vi /etc/ssh/sshd_config
 - 將PermitRootLogin這一行反註解，並且確認其選項為no。
 - 設定完畢重啟sshd以套用新規則：
 - sudo service sshd restart

```
# Logging
# obsoletes QuietMode and
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

基本指令-網路連線

□ 防火牆

- 允許8080 port與FTP連線

- sudo iptables -A INPUT -p tcp --dport 8080 -j ACCEPT

- sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT

- 允許特定IP使用ssh連線

- sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT

- sudo iptables -A INPUT -p tcp -s {IP} --dport 22 -j ACCEPT

基本指令-網路連線

□ 防火牆

○ 或直接編輯檔案：

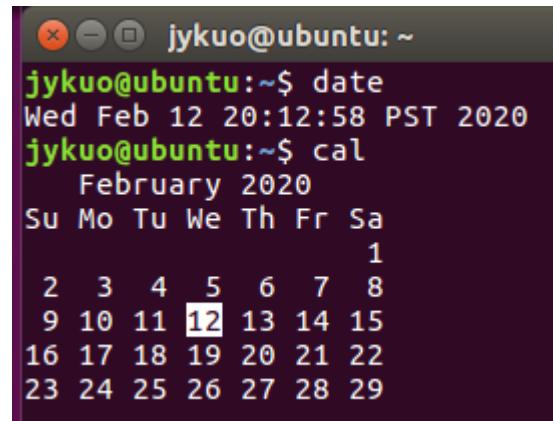
- sudo vi /etc/sysconfig/iptables
- 設定完畢重啟iptables以套用新規則：
- sudo service iptables restart

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
###新增
-A INPUT -p tcp --dport 8080 -j ACCEPT
-A INPUT -p tcp --dport 20 -j ACCEPT
-A INPUT -p tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -s                         --dport 22 -j ACCEPT
-A INPUT -p tcp -s                         --dport 22 -j ACCEPT
###
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

基本指令

□ date

- 查看日期



```
jykuo@ubuntu:~$ date
Wed Feb 12 20:12:58 PST 2020
jykuo@ubuntu:~$ cal
February 2020
Su Mo Tu We Th Fr Sa
          1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
```

□ cal

- 查看日曆

基本指令

□ 網路校時crontab。

○ sudo vi /etc/crontab

○ 新增以下內容：

➤ 30 4 * * * root /usr/sbin/ntpdate watch.stdtime.gov.tw

➤ 0 5 * * * root /usr/sbin/ntpdate time.stdtime.gov.tw &&
/usr/sbin/hwclock -w

○ 設定早上4:30校時1次，早上5:00校時1次並寫入BIOS時鐘。

基本指令

□ grep (global regular expression print)

- 查找檔案文字，全域正則表達式列印。
- 以行為單位。將文字檔案的第1行讀入緩衝區查詢，若找到匹配字符，則輸出整行。
- 常用的選項
 - i：忽略大小寫。
 - n：將結果輸出的同時，也輸出該行的行號。
 - s：沒找到匹配內容時，不顯示錯誤信息。
 - l：從多個文件中找，只輸出找到匹配內容的文件名稱。
 - h：從多個文件中找，只輸出匹配內容，不顯示文件名稱。
 - c：只輸出匹配內容的總行數
 - v：反轉找，即輸出匹配內容以外的行。

基本指令

□ 萬用字元

- Shell 底下，擁有一些特殊符號，稱為萬用字元 (wild card)。對於檔名的展開相當好用。

符號	說明
?	萬用字元，代表此處一定要有『一個字元』
*	萬用字元，代表此處可以有『0或多個字元』

Search String	Files Found
File_?	File <u>A</u> File <u>B</u>
File_??	File <u>Aa</u> File <u>Bb</u>
File_*	File File <u>A</u> File <u>AB</u> File <u>ABC</u> File <u>Denny</u> File <u>Yenjin</u>
?ile_*	<u>F</u> ile <u>f</u> ile <u>A</u> ile <u>a</u> ile <u>A</u> <u>B</u> ile <u>ABC</u> <u>b</u> ile <u>1</u> <u>C</u> ile <u>123</u>

基本指令

□ 正規表示式

符號	說明	舉例
^	行的開頭	^The : 搜尋開頭為The的內容。
\$	行的結尾	End\$: 搜尋結尾為End的內容。
[abc]	符合集合中的字	[abc] : 檔案中只要有 "a"、"b"、"c" 任一字即符合搜尋。
[a-z]、[A-Z]	符合集合範圍中的字	[a-z] : 符合 "a" 到 "z" 所有字元。 [A-Z] : 符合 "A" 到 "Z" 所有字元。 [0-9] : 符合 "0" 到 "9" 所有字元。
.	任何單一字元	file. : 符合 file1、file2， 但不符合 file10。
+	一個或多個字元	[0-9]+ : 符合所有數字字元，表示檔案中只要有數字即符合搜尋。
*	0個或多個表示式	file.* : 符合 file、file2、file10。
?	0個或一個表示式	file1?2 : 符合 file2、file12。
	符合前面或者後面	file File : 符合 file也符合 File。

基本指令

□ grep (global regular expression print)

○ 範例

- grep "canred" students, grep -n "canred" students
- grep -c "canred" students, grep -i "CanRed" students
- grep -vi "canred" students | grep -vi "eva"

○ 多文件

- grep -l "root" /etc/* , 顯示/etc目錄中所有包含有root的文件名
- grep -h "root" /etc/passwd /etc/shadow

○ 使用grep在命令輸出中找

- echo "Welcome to Taiwan" | grep "Taiwan"

○ 使用grep在變數中找

- A="Welcome to Taiwan"
- echo \$A | grep "Taiwan"

基本指令

□ grep (global regular expression print)

○ 行首，行尾匹配找

- grep '^canred' students
- grep 'canred\$' students

○ 正則表達式找

- grep '/9[0-9]' students
- grep 'c\{3,\}' students
- grep 'canred\{2\}p\$' students
- ls -l | grep '\.txt\$'

○ 使用或、與多匹配模式查找

- grep -E 'Canred|Eva' students
- grep 'Canred' students | grep "Eva"