

Ch3 Linux Network & Tools



Cite <http://www.techomag.com/>

謝明志(Jimin Hsieh)

Agenda

- 3-1 Basic Utilities
- 3-2 Set up your IP
- 3-3 SSH
- 3-4 Telnet
- 3-5 Wireshark
- 3-6 Nmap

3-1 Basic Utilities

- Local

1. # ifconfig

1.1. # ifconfig
[interface]

1.2. # ifconfig
[interface] down/up

1.2. # ifconfig
[interface] [ip]

2. # route

3. # netstat

3.1. option:"-a"

Internet connections

vs.

UNIX domain sockets

3.2. # netstat | grep
[strings]

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 JiminLab.local:ssh      JiminNB.local:46717    ESTABLISHED
udp6       0      0 localhost:47189         localhost:47189        ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node  Path
unix    2      [ ]     DGRAM      -            5888     /var/run/xrdp/xrdp_sesman_00000
```

3-1 Basic Utilities

```
root@JiminNB:~# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr f0:de:f1:e1:39:6e  
          inet addr:163.13.127.130  Bcast:163.13.127.255  Mask:255.255.255.0  
          inet6 addr: fe80::f2de:f1ff:fe1:396e/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:39940 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:36885 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:39065309 (37.2 MiB)  TX bytes:6995928 (6.6 MiB)  
          Interrupt:42 Base address:0x6000
```

```
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:16436  Metric:1  
          RX packets:1687 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1687 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:128032 (125.0 KiB)  TX bytes:128032 (125.0 KiB)
```

```
wlan0     Link encap:Ethernet  HWaddr 44:6d:57:18:55:39  
          inet addr:192.168.0.101  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::466d:57ff:fe18:5539/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:351 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:32224 (31.4 KiB)  TX bytes:6617 (6.4 KiB)
```

3-1 Basic Utilities

- Remote
 1. # ping [ip-address]: send ICMP packet
 - 1.1. option: -i [integer]
ping with specific interval
 - 1.2. option: -s [packet size]
 2. # traceroute [ip-address]: show the route
- Other
 1. # wget [IP + file]: download file from Internet

3-2 Set up your IP

1. DHCP

1.1. IP address

/etc/network/interfaces

auto [interface]

allow-hotplug [interface]

iface [interface] inet dhcp

2. Static IP

1.1. IP address

/etc/network/interfaces

auto [interface]

iface [interface] inet static

address [IP]

netmask [mask]

gateway [Gateway IP]

2.2. DNS IP address

/etc/resolve.conf

nameserver [IP]

3-3 SSH

- Secure Shell

1. ssh server: openssh-server

2. ssh client(Linux):

- 2.1. # ssh user@ip-address

- 2.2. Remote to Local: # scp [-r] user@ip-address:[file] [location of local]

- 2.3. Local to Remote: # scp [-r] [file/directoy] user@ip-address:[location of remote]

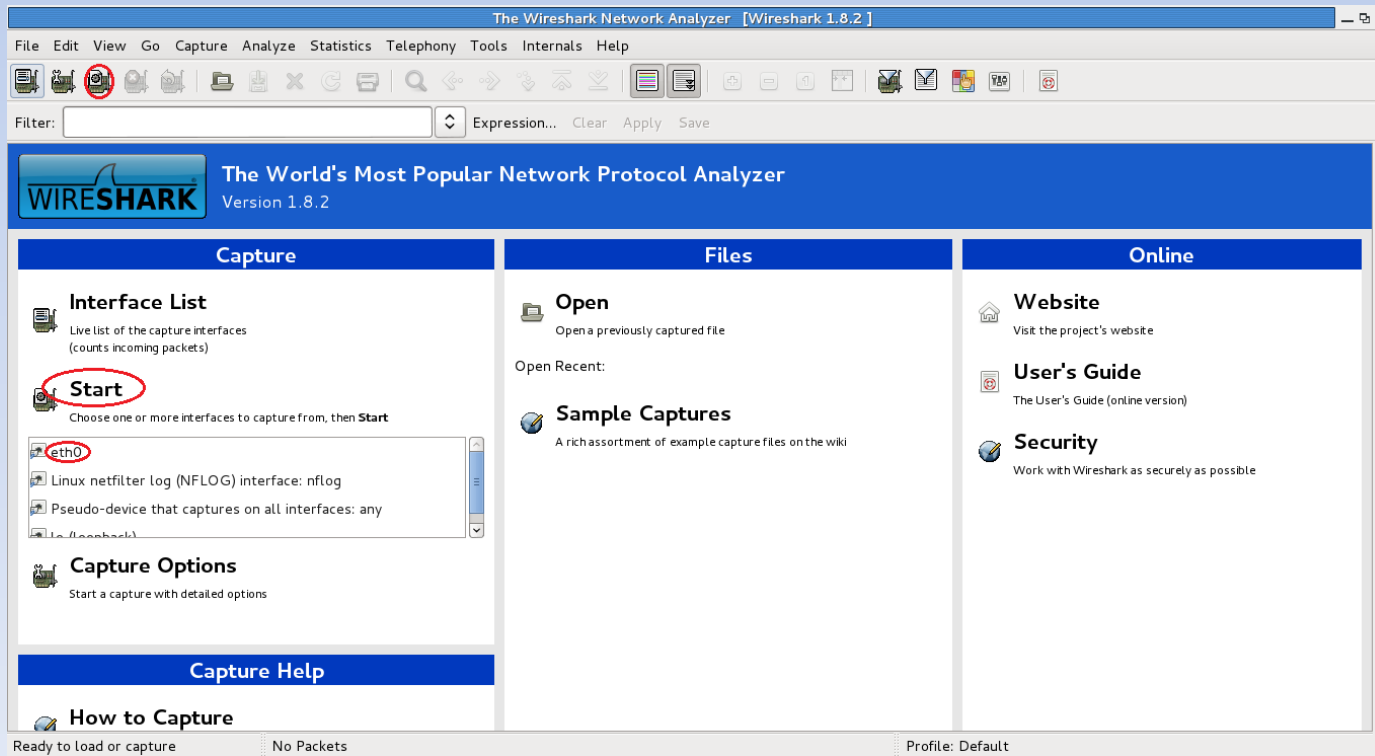
3. ssh client(Win): putty

3-4 Telnet

1. telnet server: telnetd or telnetd-ssl
2. telnet client(Linux)
 - 2.1. # telnet user@[ip-address]
 - 2.2. putty
3. telnet client(Win): putty

3-5 Wireshark

- Packet analyzer
- Using privilege of root to open in console
- # wireshark



CH3-5 Wireshark

eth0 [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
173	0.856679000	192.168.1.20	163.13.241.159	TCP	54	49260 > cslistener [ACK] Seq=1 Ack=86421 Win=64400 Len=0
174	0.857268000	163.13.241.159	192.168.1.20	TCP	1439	cslistener > 49260 [PSH, ACK] Seq=86421 Ack=1 Win=4096 Len=1385
175	0.857283000	163.13.241.159	192.168.1.20	TCP	284	cslistener > 49260 [PSH, ACK] Seq=87806 Ack=1 Win=4096 Len=230
176	0.857415000	163.13.241.159	192.168.1.20	TCP	687	cslistener > 49260 [PSH, ACK] Seq=88036 Ack=1 Win=4096 Len=633
177	0.857445000	192.168.1.20	163.13.241.159	TCP	54	49260 > cslistener [ACK] Seq=1 Ack=88036 Win=64400 Len=0
178	0.898768000	163.13.241.159	192.168.1.20	TCP	1445	cslistener > 49260 [PSH, ACK] Seq=88669 Ack=1 Win=4096 Len=1391
179	0.898799000	163.13.241.159	192.168.1.20	TCP	269	cslistener > 49260 [PSH, ACK] Seq=90060 Ack=1 Win=4096 Len=215
180	0.899247000	192.168.1.20	163.13.241.159	TCP	54	49260 > cslistener [ACK] Seq=1 Ack=90275 Win=64400 Len=0
181	0.899882000	163.13.241.159	192.168.1.20	TCP	1447	cslistener > 49260 [PSH, ACK] Seq=90275 Ack=1 Win=4096 Len=1393
182	0.899901000	163.13.241.159	192.168.1.20	TCP	362	cslistener > 49260 [PSH, ACK] Seq=91668 Ack=1 Win=4096 Len=308
183	0.899906000	163.13.241.159	192.168.1.20	TCP	147	cslistener > 49260 [PSH, ACK] Seq=91976 Ack=1 Win=4096 Len=93

Frame 182: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface 0

Ethernet II, Src: PlanexCo_d9:20:97 (00:90:cc:d9:20:97), Dst: CadmusCo_f6:4c:97 (08:00:27:f6:4c:97)

Internet Protocol Version 4, Src: 163.13.241.159 (163.13.241.159), Dst: 192.168.1.20 (192.168.1.20)

Transmission Control Protocol, Src Port: cslistener (9000), Dst Port: 49260 (49260), Seq: 91668, Ack: 1, Len: 308

Data (308 bytes)

```
0000 08 00 27 f6 4c 97 00 90 cc d9 20 97 08 00 45 00  ..'.L... ..E.
0010 01 5c 3d 00 00 00 7d 06 a9 32 a3 0d f1 9f c0 a8  .\=...}. .2.....
0020 01 14 23 28 c0 6c 04 7f 22 48 1c 5f 3a 2d 50 18  .#(.l.. "H._:~P.
0030 10 00 d0 fc 00 00 04 10 03 1b 81 6f 3a 6b 04 10  .....:o:k..
0040 00 1d 81 11 64 0c 04 10 03 1d 81 df 7b 73 0d 10  ....d... ..{s..
```

File: "/tmp/wireshark_eth0_20131... Packets: 1544 Displayed: 1544 Marked: 0 Dropped: 0 Profile: Default

CH3-5 Wireshark

Filter: tcp, udp, icmp...etc

The image shows the Wireshark 1.8.2 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. The filter bar at the top of the packet list shows 'Filter: tcp' with a green background. The packet list table below shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by TCP. The bottom pane shows the details of the selected packet (No. 1925), displaying the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers.

No.	Time	Source	Destination	Protocol	Length	Info
1919	49.999401000	192.168.1.102	69.28.148.72	TCP	66	33271 > http [ACK] Seq=1 Ack=200262 Win=386 Len=0 TSval=4505868 TSecr=2978149145
1920	50.026987000	163.13.243.116	192.168.1.102	TCP	199	irdmi2 > 48465 [PSH, ACK] Seq=27564 Ack=1 Win=513 Len=133 TSval=39298643 TSecr=4505868
1921	50.027040000	192.168.1.102	163.13.243.116	TCP	66	48465 > irdmi2 [ACK] Seq=1 Ack=27697 Win=1357 Len=0 TSval=4505875 TSecr=39298643
1922	50.062772000	69.28.148.72	192.168.1.102	HTTP	317	Continuation or non-HTTP traffic
1923	50.062894000	192.168.1.102	69.28.148.72	TCP	66	33271 > http [ACK] Seq=1 Ack=200513 Win=386 Len=0 TSval=4505884 TSecr=2978149208
1924	50.123853000	69.28.148.72	192.168.1.102	HTTP	551	Continuation or non-HTTP traffic
1925	50.123903000	192.168.1.102	69.28.148.72	TCP	66	33271 > http [ACK] Seq=1 Ack=200998 Win=386 Len=0 TSval=4505899 TSecr=2978149271
1926	50.143715000	163.13.243.113	192.168.1.102	TCP	1375	irdmi2 > 45951 [PSH, ACK] Seq=70147 Ack=1 Win=396 Len=1309 TSval=107241920 TSecr=4505904
1927	50.143742000	192.168.1.102	163.13.243.113	TCP	66	45951 > irdmi2 [ACK] Seq=1 Ack=71456 Win=1455 Len=0 TSval=4505904 TSecr=107241920
1928	50.186747000	69.28.148.72	192.168.1.102	HTTP	231	Continuation or non-HTTP traffic
1929	50.186793000	192.168.1.102	69.28.148.72	TCP	66	33271 > http [ACK] Seq=1 Ack=201163 Win=386 Len=0 TSval=4505915 TSecr=2978149334

Frame 1925: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: WistronI_e1:39:6e (f0:de:f1:e1:39:6e), Dst: PlanexCo_d9:20:97 (00:90:cc:d9:20:97)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 69.28.148.72 (69.28.148.72)
Transmission Control Protocol, Src Port: 33271 (33271), Dst Port: http (80), Seq: 1, Ack: 200998, Len: 0

3-6 Nmap

Nmap (Network mapper) – Network Scanner

- # nmap [IP]
 1. option: "-O" enable OS detect
nmap -O [IP]
 2. option: "-sn"/ "-sP" scan PC through ICMP
nmap -sn 192.168.1.0/24
 3. option: "-sT" scan TCP port
nmap -sT [IP]
 4. option: "-sU" scan UDP port

3-6 Nmap

```
root@JiminLab:~# nmap -O www.facebook.com
```

```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-11-06 09:11 CST  
Nmap scan report for www.facebook.com (31.13.68.8)  
Host is up (0.027s latency).
```

```
rDNS record for 31.13.68.8: edge-star-shv-01-hkg1.facebook.com
```

```
Not shown: 997 filtered ports
```

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

843/tcp	closed	unknown
---------	--------	---------

```
Device type: storage-misc
```

```
Running (JUST GUESSING): Linksys Linux 2.6.X (88%)
```

```
OS CPE: cpe:/o:linux:kernel:2.6.18
```

```
Aggressive OS guesses: Linux 2.6.18 (88%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds
```

```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-11-06 09:22 CST
```

```
Nmap scan report for [REDACTED]
```

```
Host is up (0.0057s latency).
```

```
Not shown: 995 filtered ports
```

PORT	STATE	SERVICE
------	-------	---------

135/tcp	open	msrpc
---------	------	-------

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

3389/tcp	open	ms-wbt-server
----------	------	---------------

49155/tcp	open	unknown
-----------	------	---------

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: general purpose
```

```
Running: Microsoft Windows Vista
```

```
OS CPE: cpe:/o:microsoft:windows_vista::sp1:home premium
```

```
OS details: Microsoft Windows Vista Home Premium SP1
```

```
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
```

Q&A

Thanks for you attentions!