리눅스 utility

1. top
   >>시스템의 전반적인 상황 확인

```
[s21900102@peace:~$ top

top - 17:37:28 up 4 days,  4:07,  7 users,  load average: 17.60, 17.52, 17.47
Tasks: 580 total,  18 running, 340 sleeping,  10 stopped,   0 zombie
%Cpu(s): 33.6 us,  9.0 sy,  0.0 ni, 57.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
KiB Mem : 32820496 total, 12480156 free, 15129980 used,  5210360 buff/cache
KiB Swap: 33438716 total, 33438204 free,      512 used. 17081928 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
22381 s218005+  20   0    4220    904    824 R 100.0  0.0   3185:00 ./a.out
26030 s218005+  20   0    4220    908    828 R 100.0  0.0   3161:01 ./a.out
26126 s218005+  20   0    4220    904    824 R 100.0  0.0   3161:38 ./a.out
26154 s218005+  20   0    4220    896    816 R 100.0  0.0   3159:14 ./a.out
26296 s218005+  20   0    4220    896    820 R 100.0  0.0   3160:12 ./a.out
40530 s214007+  20   0    4356     76      0 R 100.0  0.0   3307:25 ./a.out gr+
40642 s214007+  20   0    4356     72      0 R 100.0  0.0   3306:49 ./a.out gr+
40846 s214007+  20   0    4356     72      0 R 100.0  0.0   3305:25 ./a.out gr+
 2205 s214007+  20   0    4356     72      0 R 100.0  0.0   3295:01 ./a.out gr+
11297 s218005+  20   0    4220     72      0 R 100.0  0.0   3246:31 ./a.out
13035 s214007+  20   0    4356     76      0 R 100.0  0.0   2988:18 ./a.out gr+
22624 s218005+  20   0    4220    904    824 R 100.0  0.0   3183:29 ./a.out
25782 s218005+  20   0    4220    904    824 R 100.0  0.0   3160:53 ./a.out
26049 s218005+  20   0    4220    976    900 R 100.0  0.0   3161:17 ./a.out
36724 s214007+  20   0    4352     76      0 R 100.0  0.0   3329:03 ./a.out qw+
```

   cpu, 메모리 등의 정보를 알 수 있다.
   옵션으로는 -d 2, -q 이 있는데 이 옵션을 사용하면 초단위로 또는 실시간으로
   시스템의 정보가 업데이트 되어 출력된다.

2. ifconfig
   >>네트워크 인터페이스 구성 확인

```
[s21900102@peace:~$ ifconfig
enp129s0f0 Link encap:Ethernet  HWaddr 0c:c4:7a:e1:87:5a
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:fb320000-fb33ffff

enp129s0f1 Link encap:Ethernet  HWaddr 0c:c4:7a:e1:87:5b
          inet addr:203.252.112.10  Bcast:203.252.112.63  Mask:255.255.255.192
          inet6 addr: fe80::2dd:2812:b125:efe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2872940 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2122603 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1006640304 (1.0 GB)  TX bytes:861302102 (861.3 MB)
          Memory:fb300000-fb31ffff

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

다음과 같은 출력을 해준다 여기서 각각의 문단의 앞으로 나와있는 것은 네트워크 인터페이스 이다.
ifconfig를 이용하면 네트워크 인터페이스를 설정할 수 있는데,
나는 이 peace서버의 host가 아니라서 설정이 허락되지 않는다.
2. ip

```
[s21900102@peace:/etc$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp129s0f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN
group default qlen 1000
    link/ether 0c:c4:7a:e1:87:5a brd ff:ff:ff:ff:ff:ff
3: enp129s0f1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP grou
p default qlen 1000
    link/ether 0c:c4:7a:e1:87:5b brd ff:ff:ff:ff:ff:ff
    inet 203.252.112.10/26 brd 203.252.112.63 scope global enp129s0f1
       valid_lft forever preferred_lft forever
    inet6 fe80::2dd:2812:b125:efe/64 scope link
       valid_lft forever preferred_lft forever
```

다음과 같이 ip addr show를 하면 네트워크 인터페이스의 ip주소를 확인할 수 있다.
show를 생략하고 명령해도 같다.

3. netstat
네트워크 접속, 라우팅 테이블, 네트워크 인터페이스 통계정보 출력

```
[s21900102@peace:/etc$ netstat --help
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
        -a, --all, --listening   display all sockets (default: connected)
        -o, --timers             display timers
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB

  <Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
```

netstat의 사용법은 다음과 같다.

```
[s21900102@peace:/etc$ netstat -antplF
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:15215         0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:15216         0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:15218         0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
-
tcp        0      0 203.252.112.10:22       172.18.201.1:51009      ESTABLISHED
-
tcp        0      0 203.252.112.10:22       203.252.105.189:53452   ESTABLISHED
-
tcp        0      0 203.252.112.10:22       203.252.121.216:57430   ESTABLISHED
-
tcp        0      0 203.252.112.10:22       172.18.201.1:8310       ESTABLISHED
-
tcp        0      0 203.252.112.10:22       203.252.105.188:55922   ESTABLISHED
-
tcp        0    352 203.252.112.10:22       172.18.201.1:51545      ESTABLISHED
-
tcp        0      0 203.252.112.10:22       172.18.201.1:59913      ESTABLISHED
-
tcp        0      0 203.252.112.10:22       203.252.117.201:40870   ESTABLISHED
-
```

다음과 같이 -antplF를 하면 각 프로토콜 종류와 해당 process가 주고 받는 바이트, local주소와 목적지주소, 포트의 상태를 출력하여 준다.
여기서 LISTEN은 대기 하고 있는 포트로 열려있는 포트이다. ESTABLISHED는 이미 연결이 완료된 포트이다.

3. host

```
[s21900102@peace:/etc$ host naver.com
naver.com has address 210.89.160.88
naver.com has address 125.209.222.142
naver.com has address 210.89.164.90
naver.com has address 125.209.222.141
naver.com mail is handled by 10 mx1.naver.com.
naver.com mail is handled by 10 mx2.naver.com.
naver.com mail is handled by 10 mx3.naver.com.
[s21900102@peace:/etc$ host hisnet.handong.edu
hisnet.handong.edu has address 203.252.97.22
[s21900102@peace:/etc$ host handong.edu
handong.edu has address 211.253.29.84
handong.edu mail is handled by 1 ASPMX.L.GOOGLE.COM.
handong.edu mail is handled by 5 ALT1.ASPMX.L.GOOGLE.COM.
handong.edu mail is handled by 10 ASPMX3.GOOGLEMAIL.COM.
handong.edu mail is handled by 10 ASPMX2.GOOGLEMAIL.COM.
handong.edu mail is handled by 5 ALT2.ASPMX.L.GOOGLE.COM.
```

다음은 host명령어의 사용 예이다.

다음과 같이 host 도메인 네임을 하면 그 ip주소 뿐만아니라 하위 호스트명도 조회할 수 있다.

4. hostname

```
[s21900102@peace:/etc$ hostname
peace
```

이 명령어는 이 서버의 호스트 명을 알려준다.
--ip 옵션 : 호스트의 ip주소를 알려준다.

```
[s21900102@peace:/etc$ hostname --ip
127.0.1.1
```

--yp 옵션 : 호스트의 도메인 명을 출력하는데 지금 peace에서는 로컬 도메인 명이 설정되어있지 않다.

```
[s21900102@peace:/etc$ hostname --yp
hostname: Local domain name not set
```

--version : 호스트네임의 버전정보를 출력한다.

```
[s21900102@peace:/etc$ hostname --version
hostname 3.16
```

5. ethtool

```
[s21900102@peace:/etc$ ethtool enp129s0f1
Settings for enp129s0f1:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        MDI-X: off (auto)
Cannot get wake-on-lan settings: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

다음과 같이 ethtool 인터페이스명을 하면 정보가 출력이 된다. 보는 것과 같이 speed값과 duplex값(Half/Full) = 전송모드 포트 등의 정보가 출력이 된다.
-s 옵션 등을 이용하면 이러한 정보를 수정할 수가 있다.

6. traceroute
   컴퓨터에서 목적지 서버로 가는 네트워크 경로를 확인해준다.

```
[s21900102@peace:/etc$ traceroute handong.edu
traceroute to handong.edu (211.253.29.84), 30 hops max, 60 byte packets
 1  203.252.112.1 (203.252.112.1)  1.595 ms  2.588 ms  3.563 ms
 2  172.18.201.1 (172.18.201.1)  0.204 ms  0.195 ms  0.185 ms
 3  203.251.71.133 (203.251.71.133)  0.516 ms  0.515 ms  0.535 ms
 4  * * *
 5  * * *
 6  112.190.135.181 (112.190.135.181)  0.481 ms  0.492 ms  0.527 ms
 7  112.190.175.229 (112.190.175.229)  2.628 ms  2.649 ms  2.620 ms
 8  * * *
 9  112.174.63.50 (112.174.63.50)  11.309 ms 112.174.62.194 (112.174.62.194)  11
.895 ms 112.174.62.242 (112.174.62.242)  11.588 ms
10  112.188.240.210 (112.188.240.210)  7.141 ms  5.741 ms 112.188.240.206 (112.1
88.240.206)  7.253 ms
11  211.55.34.162 (211.55.34.162)  7.106 ms  6.917 ms 211.55.34.166 (211.55.34.1
66)  6.218 ms
12  211.253.15.26 (211.253.15.26)  7.477 ms 211.253.15.30 (211.253.15.30)  7.988
 ms 211.253.15.22 (211.253.15.22)  7.690 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
```

   TTL(Time to live)가 짧은 UDP probe 패킷을 보내고 게이트웨이에서 ICMP"time exceeded" 응답을 받으면 IP 패킷이 인터넷 호스트까지 가는 경로를 파악함.
   시도 횟수는 기본 30으로 30줄 까지 나온다. (-m으로 변경) 만약 5초의 타임아웃(-w로 변경) 동안 응답이 없으면 *이 출력됨

7. nslookup
   DNS(Domain name Server)에 질문하는 명령어

```
[s21900102@peace:~$ nslookup handong.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   handong.edu
Address: 211.253.29.84
```

   handong.edu 의 ip주소를 출력한다.
   DNS Record type

```
[s21900102@peace:~$ nslookup -type=a handong.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   handong.edu
Address: 211.253.29.84
```

   다음 예시는 type을 a로 하여 IPv4만 출력하도록 하였다.
   이 외에도 Type에는

a	IPv4
aaaa	IPv6
MX	메일서버
NS	네임서버
SOA	마스터네임서버
SRV	정방향
txt	텍스트
PTR	역방향

등의 타입이 있다.

8. ping

```
[s21900102@peace:~$ ping -c 3 handong.edu
PING handong.edu (211.253.29.84) 56(84) bytes of data.
j
--- handong.edu ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2043ms
```

ping은 외부 호스트 서버가 네트워크상으로 접근가능한지 확인 해 본다.
handong.edu 의 경우에는 ping을 차단해 둔 것 같다. 그래서 위와 같이 결과를 받지 못하였다.