




제 3장 우분투 관리

- ✓ 3-1 파일 시스템
- ✓ 3-2 패키지 관리
- ✓ 3-3 사용자관리
- ✓ 3-4 반복 작업 자동화하기
- ✓ 3-5 네트워크 관리

 한국기술교육대학교

 컴퓨터공학부 박진우 책임기술연구원 2405호



네트워크 관리

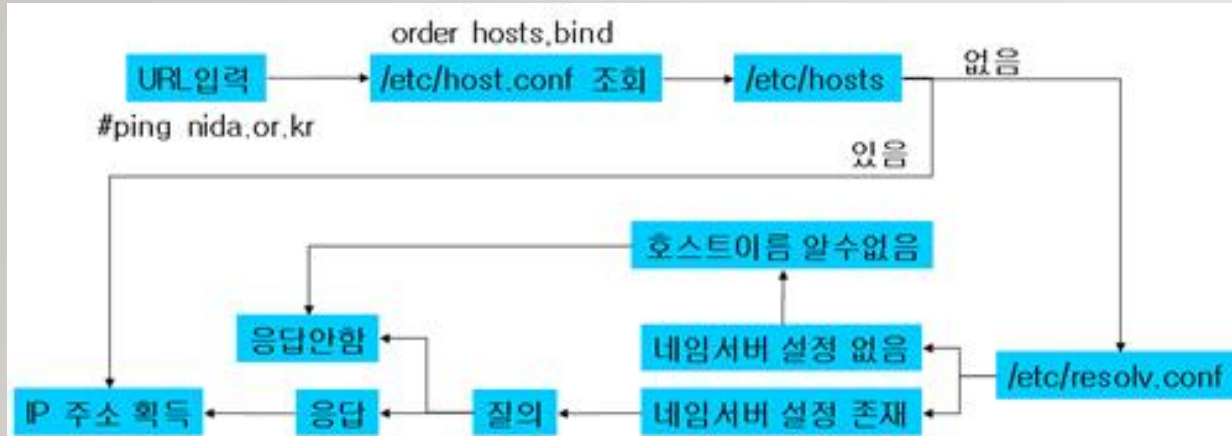
● 호스트명과 IP주소

- ◆ 호스트명(Hostname)은 **네트워크에 연결된 장치(컴퓨터, 파일 서버, 복사기 등)들에 부여된 고유한 이름**이다. 특히 인터넷에서는 월드 와이드 웹, 전자 우편, 유즈넷 등에서 호스트명을 흔히 사용하며, 도메인 이름과 유사하지만 엄밀하게는 더 넓은 의미를 가지고 있다.
- ◆ 호스트명은 보통 **사람이 읽고 이해할 수 있는 이름으로 지어지며**, 흔히 IP 주소나 MAC 주소와 같은 기계적인 이름 대신 쓸 수 있다. 호스트명은 NIS, DNS, SMB 등의 여러 체계에서 사용되기 때문에 네트워크에 따라서 같은 컴퓨터에 배당된 호스트명이 달라질 수도 있다.
- ◆ IP 주소(Internet Protocol address, 표준어: 인터넷규약주소)는 컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신을 하기 위해서 사용하는 특수한 번호이다.
- ◆ IP 주소는 LAN이나 WAN, 인터넷에서만 사용되는 전화번호라고 생각할 수 있다. 한편, 이런 번호는 사람이 외우기 어렵기 때문에, 전화번호부와 같은 역할을 하는 서비스가 필요하다. DNS가 이런 역할을 하며 이런 서비스를 "도메인 이름 분석(domain name resolution)" 혹은 "이름 분석(name resolution)"이라고 한다.

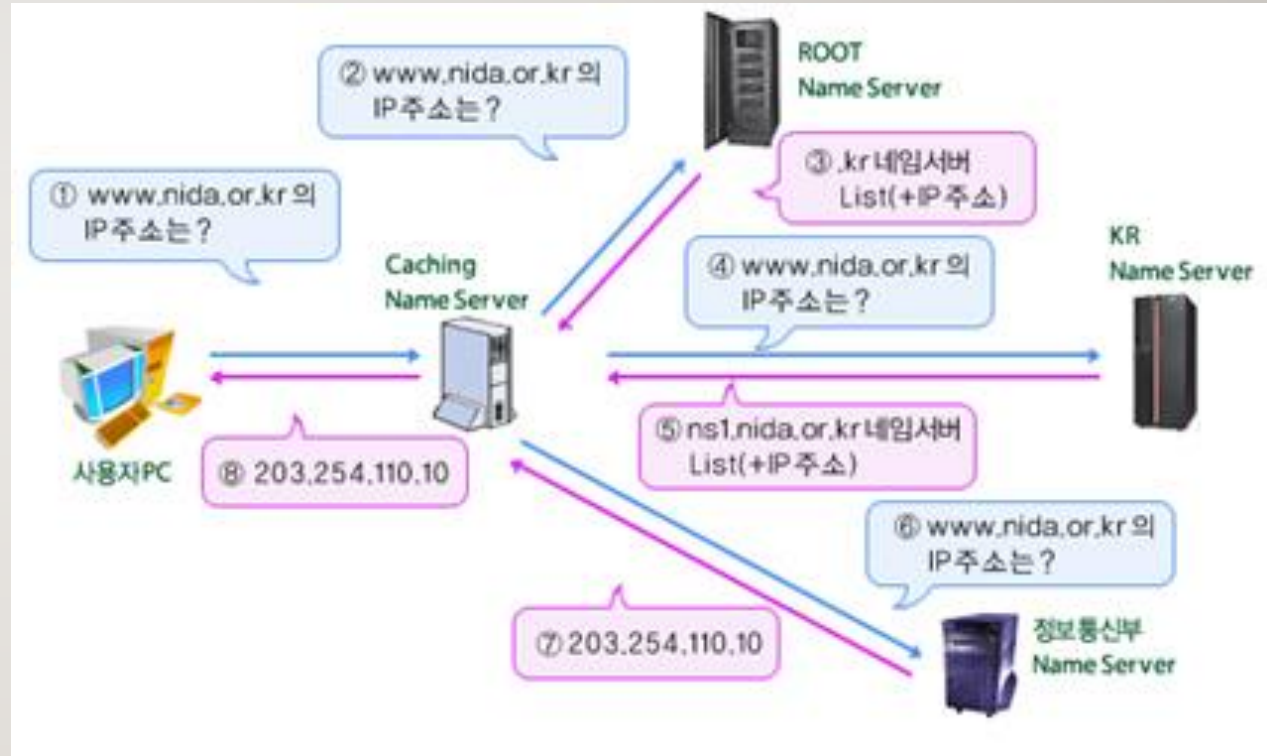


네트워크 관리

• 호스트 검색 과정



- 우분투에서 URL을 입력하게 되면 위 그림과 같은 절차에 따라서 호스트 검색이 이루어지게 된다.
- 여기서 "질의"에 해당하는 것을 다시 보면 오른쪽 그림과 같다.





네트워크 관리

● 네트워크 관리 명령어

◆ ping

핑(PING, Packet Internet Groper)은 특정한 인터넷 호스트의 주소로 그 주소가 응답을 할 수 있는지 확인하는데 사용되는 명령어이다.

- ◆ 가장 기본적인 인터넷 프로토콜로 ICMP(Internet Control Message Protocol, 인터넷 제어 메시지 프로토콜) 프로토콜을 기반으로 사용하며 이때 원격의 호스트가 사용 가능상태인지를 ICMP 프로토콜을 보내고 다시 되받아서 확인 할 수 있다.

● ping [host , ip주소]

◆ 옵션으로는

-c 횟수 : 지정한 횟수만큼 icmp packet 을 송신

-i 간격 : 지정간격마다 icmp packet 을 송신 (default는 1초)

- ◆ ip로는 소통이 가능하지만 호스트명으로는 소통이 안될경우 DNS가 원인일 가능성이 있다. 이 경우 DNS서버의 가동상태 확인과

- ◆ /etc/resolv.conf 파일의 설정을 확인해 본다.



네트워크 관리

• ping 차단방법

- ◆ /proc/sys/net/ipv4 디렉터리는 네트워크 관련정보를 가지고 있다.
 - # echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all ==> 바로 적용되어 ping 차단
 - # echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts ==> Dos공격에 효과적 대처
- ◆ /etc/sysctl.conf 파일 맨 아래에 다음과 같은 내용을 추가해주고 reboot 하거나 network을 다시 시작해 주면 ping을 영구적으로 차단할 수 있다.

```
net.ipv4.icmp_echo_ignore_all = 1
```

```
# echo 64 > /proc/sys/net/ipv4/ip_default_ttl ==> ip패킷의 생존시간을 1~255까지 조정가능
```

- ◆ sysctl net.ipv4.ip_forward ==> sysctl 명령어로 ip_forward 상태 확인
- ◆ sysctl 명령을 사용할 경우에는 /proc/sys/ 까지는 생략하고 「/」대신「.»으로 표기한다.

```
net.ipv4.ip_forward = 0
```

```
# sysctl -w net.ipv4.ip_forward=1
```

```
root@study: ~  
root@study:~# sysctl net.ipv4.ip_forward  
net.ipv4.ip_forward = 0  
root@study:~#  
root@study:~# sysctl -w net.ipv4.ip_forward=1  
net.ipv4.ip_forward = 1  
root@study:~#
```



네트워크 관리

- **traceroute**

라우팅 경로를 찾는 명령어로 traceroute 를 위해서는 ICMP type 11(time-exceeded) 가 필터링 되어서는 결과를 얻을 수 없다.

이 명령을 이용하여 지정host까지 packet가 전해지는 경로를 표시하여 네트워크 경로상의 장애발생위치를 추정할 수 있다.

- ◆ **traceroute [host , ip주소]**

- F : ip패킷을 분할하지 않는다
- g 게이트웨이 : 경유하는 gw지정 (최대 8서버 지정 가능)
- I : icmp echo를 이용
- T : TCP SYN을 이용
- m 최대값 : 경유하는 최대 host 수를 지정
- n : host 명을 해결하지않고 IP주소로 표시
- p 포트 : 이용하는 port 를 지정
- r : routing table 을 무시
- s ip주소 : 지정한 IP 주소에서 경로를 조사
- v : 상세히 표시
- w 시간 : time out 시간 지정
- x : icmp를 checksum으로 평가
- z 시간 : 경로를 체크하는 시간 간격 지정

```
root@study: ~  
root@study:~# traceroute -T www.hosting.kr  
traceroute to www.hosting.kr (110.45.158.195), 30 hops max, 60 byte packets  
 1  192.168.214.2 (192.168.214.2)  0.105 ms  0.111 ms  0.067 ms  
 2  hosting.co.kr (110.45.158.195)  17.593 ms  17.633 ms  16.620 ms  
root@study:~#
```



네트워크 관리



- **host**

dns 서버를 사용해 호스트와 도메인에 관한 정보를 표시한다.

- ◆ **host [host , ip주소]**

```
root@study: ~  
root@study:~# host jtbtc.join.com  
jtbtc.join.com has address 211.218.152.124  
root@study:~#  
root@study:~# host www.koreatech.ac.kr  
www.koreatech.ac.kr has address 220.68.95.227  
root@study:~#
```



네트워크 관리



- **hostname**

호스트명을 출력하거나 호스트의 이름을 변경할 수 있다. 호스트명은 /etc/hostname 파일에 저장된다.

- ◆ **hostname [옵션] 호스트명 확인**

- v : 호스트네임을 출력
- d : DNS 도메인 네임을 출력
- f : 완전한 호스트 네임 (FQDN)을 출력
- a : 호스트 네임에 대한 Alias이름을 출력
- i : 호스트 네임에 대한 IP주소를 출력

hostname [호스트명] 호스트명 지정, 변경



네트워크 관리

- netstat

netstat 명령어는 시스템이 외부와의 연결이 어떻게 되어 있는지를 출력해주는 프로그램입니다. 이를 확인해 봄으로써 어떠한 서비스가 동작하고 있는지 판단 할 수 있다. 즉, 네트워크 포트(TCP,UDP) 오픈상태를 확인한다.

```
root@study: ~  
root@study:~# netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost:mysql        *:.*                    LISTEN  
tcp        0      0 *:ssh                  *:.*                    LISTEN  
tcp        0      0 192.168.214.128:50914  privet.canonical.c:http ESTABLISHED  
tcp        0      0 192.168.214.128:37074  ec2-52-42-115-213:https ESTABLISHED  
tcp        0      0 192.168.214.128:34600  61.37.150.148:https    ESTABLISHED  
tcp        0      0 192.168.214.128:39676  117.18.237.29:http     ESTABLISHED  
tcp        0      0 192.168.214.128:46922  203.233.88.88:http     ESTABLISHED  
tcp        0      0 192.168.214.128:50912  privet.canonical.c:http ESTABLISHED  
tcp        0      0 192.168.214.128:45294  203.233.96.54:https    TIME_WAIT  
tcp        0      0 192.168.214.128:34602  61.37.150.148:https    TIME_WAIT  
tcp        0      0 192.168.214.128:46920  203.233.88.88:http     ESTABLISHED  
tcp        0      0 192.168.214.128:50916  privet.canonical.c:http TIME_WAIT  
tcp        0      0 192.168.214.128:39698  117.18.237.29:http     ESTABLISHED  
tcp        0      0 192.168.214.128:37072  ec2-52-42-115-213:https ESTABLISHED  
tcp        0      0 192.168.214.128:45296  203.233.96.54:https    ESTABLISHED  
tcp        0      0 192.168.214.128:41630  ec2-52-34-245-108:https ESTABLISHED  
tcp        0      0 192.168.214.128:39672  117.18.237.29:http     TIME_WAIT  
tcp        0      0 192.168.214.128:57190  server-54-230-249:https TIME_WAIT  
tcp        0      0 192.168.214.128:40812  nrt12s15-in-f3.1e1:http ESTABLISHED  
tcp        0      0 192.168.214.128:40756  ec2-50-112-172-87:https ESTABLISHED  
tcp        0      0 192.168.214.128:45296  203.233.96.54:https    ESTABLISHED
```



네트워크 관리

• netstat [옵션] 자세한 사항은 교재 참조. p235

- a : 모든 tcp/udp , port 정보를 출력
- c : 상황을 1초마다 리얼타임으로 출력
- i : 네트워크 인터페이스의 상태 출력
- l : 접속 대기중(LISTEN)상태의 소켓만 출력
- n : ip와 port번호를 숫자로 출력
- p : pid 와 프로세스명 출력
- r : routing table 을 표시 ==> # route
- t : TCP port만 표시
- u : UDP port만 표시

```
root@study: ~  
root@study:~# netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost:mysql         *:*                     LISTEN  
tcp        0      0 *:ssh                   *:*                     LISTEN  
tcp        0      0 192.168.214.128:50914   privet.canonical.c:http ESTABLISHED  
tcp        0      0 192.168.214.128:37074   ec2-52-42-115-213:https ESTABLISHED  
tcp        0      0 192.168.214.128:34600   61.37.150.148:https     ESTABLISHED  
tcp        0      0 192.168.214.128:39676   117.18.237.29:http      ESTABLISHED  
tcp        0      0 192.168.214.128:46922   203.233.88.88:http      ESTABLISHED  
tcp        0      0 192.168.214.128:50912   privet.canonical.c:http ESTABLISHED  
tcp        0      0 192.168.214.128:45294   203.233.96.54:https     TIME_WAIT  
tcp        0      0 192.168.214.128:34602   61.37.150.148:https     TIME_WAIT  
tcp        0      0 192.168.214.128:46920   203.233.88.88:http      ESTABLISHED  
tcp        0      0 192.168.214.128:50916   privet.canonical.c:http TIME_WAIT  
tcp        0      0 192.168.214.128:39698   117.18.237.29:http      ESTABLISHED  
tcp        0      0 192.168.214.128:37072   ec2-52-42-115-213:https ESTABLISHED  
tcp        0      0 192.168.214.128:45296   203.233.96.54:https     ESTABLISHED  
tcp        0      0 192.168.214.128:41630   ec2-52-34-245-108:https ESTABLISHED  
tcp        0      0 192.168.214.128:39672   117.18.237.29:http      TIME_WAIT  
tcp        0      0 192.168.214.128:57190   server-54-230-249:https  TIME_WAIT  
tcp        0      0 192.168.214.128:40812   nrt12s15-in-f3.1e1:http ESTABLISHED  
tcp        0      0 192.168.214.128:40756   ec2-50-112-172-87:https ESTABLISHED  
tcp        0      0 192.168.214.128:45296   203.233.96.54:https     ESTABLISHED
```




네트워크 관리



- **route**

IP routing table 정보를 보거나, routing table을 처리한다.

옵션 없이 사용하면 라우팅 테이블의 현재 내용을 볼 수 있고, add나 del을 사용해서 라우팅 테이블을 수정한다.

`route add [xnet|-host] target [netmask <Nm>] [gw Gw] dev <If>`

`route del [-net|-host] target [gw Gw] [netmask Nw] [[dev] If]`

`route add default gw <Gw> dev <If>`

add : route 추가

del : route 삭제

target : network 또는 host의 목적지

-e : netstat format으로 routing table을 출력한다.

```
root@study: ~
root@study:~# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          192.168.214.2  0.0.0.0         UG    0      0      0 ens33
link-local       *              255.255.0.0     U     1000   0      0 ens33
192.168.214.0    *              255.255.255.0   U      0      0      0 ens33
root@study:~#
```



네트워크 관리

- nslookup

- ◆ 도메인 네임서버에 질의를 할 수 있도록 해주는 프로그램
 - ◆ 도메인 네임 서버가 가지고 있는 정보를 검색하고, 도메인 네임 서버가 올바르게 동작하고 있는지를 확인한다.
- 시스템에서 지정한 네임서버가 아닌 다른 네임서버를 이용할 경우에는 -l 옵션을 사용하여 서버를 지정해 준다.
- ◆ nslookup www.daum.net -l 220.68.64.1

```
root@study: ~
root@study:~# nslookup www.koreatech.ac.kr
Server:      192.168.214.2
Address:     192.168.214.2#53

Non-authoritative answer:
Name:   www.koreatech.ac.kr
Address: 220.68.95.227

root@study:~#
root@study:~# nslookup www.naver.com
Server:      192.168.214.2
Address:     192.168.214.2#53

Non-authoritative answer:
www.naver.com canonical name = www.naver.com.nheos.com.
Name:   www.naver.com.nheos.com
Address: 125.209.222.142
Name:   www.naver.com.nheos.com
Address: 125.209.222.141

root@study:~#
```




네트워크 관리

- **dig (Domain Information Groper)**

- ◆ DNS 네임서버구성과 도메인 설정이 완료된 후, 인터넷 일반사용자의 입장에서 설정한 도메인네임에 대한 DNS 질의응답이 정상적으로 이루어지는지를 확인 점검하는 경우에 사용한다.

- 왜 nslookup이 아니라 dig을 사용해야 하나?

- ◆ nslookup에 비해 dig이 DNS의 추가표준사항을 충실히 반영한 진단도구이다.
- ◆ BIND DNS의 배포처인 ISC(Internet Systems Consortium)은 nslookup은 향후 배포 패키지에서 제외할 예정이며, dig을 사용하기를 권고하였다.



네트워크 관리

- dig [@server] [name] [type]

옵 션	설 명
server	DNS 질의를 할 대상 네임서버 네임서버의 도메인네임(domain name) 또는IP 주소지정 디폴트동작: 지정하지 않은 경우 시스템 resolv.conf 파일의 네임서버사용 시스템 resolv.conf에 네임서버 미지정시, localhost 사용
name	질의대상도메인네임 DNS 패킷 Question Section의 QName에 지정될 질의 대상 도메인 네임 디폴트동작 : 지정하지 않은 경우 루트도메인(.)에 대해서 질의
type	질의 타입 DNS 패킷 Question Section의 QType에 지정되는 질의 대상 RR 타입 디폴트동작: 지정하지 않은 경우 name이 지정되지 않은 경우: 루트도메인(.)의NS 타입질의 name이 지정된경우: 지정된 도메인네임의 A 타입질의



네트워크 관리

- dig 예

- ◆ ig koreatech.ac.kr ==>

- ◆ dig koreatech.ac.kr ns ==>

- ◆ dig @ns.flykorea.kr flykorea.kr axfr



네트워크 관리

```
root@study: ~  
root@study:~# dig www.koreatech.ac.kr  
  
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.koreatech.ac.kr  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58518  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096  
;; QUESTION SECTION:  
;www.koreatech.ac.kr.          IN      A  
  
;; ANSWER SECTION:  
www.koreatech.ac.kr.  5      IN      A      220.68.95.227  
  
;; Query time: 2016 msec  
;; SERVER: 192.168.214.2#53(192.168.214.2)  
;; WHEN: Thu Dec 08 03:24:24 KST 2016  
;; MSG SIZE rcvd: 64  
  
root@study:~#
```

```
root@study: ~  
root@study:~# dig www.koreatech.ac.kr ns  
  
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.koreatech.ac.kr ns  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8416  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 512  
;; QUESTION SECTION:  
;www.koreatech.ac.kr.          IN      NS  
  
;; AUTHORITY SECTION:  
koreatech.ac.kr.  5      IN      SOA      ns.kut.ac.kr. please_set_email.a  
bsolutely.nowhere. 399 10800 3600 1296000 900  
  
;; Query time: 23 msec  
;; SERVER: 192.168.214.2#53(192.168.214.2)  
;; WHEN: Thu Dec 08 03:30:30 KST 2016  
;; MSG SIZE rcvd: 126  
  
root@study:~#
```




네트워크 관리

• whois

- ◆ whois라는 도구는 IP 정보를 찾아볼 때 사용하는 도구입니다. 텔넷에서 접속한 상태에서 whois 명령을 내리면 원하는 도메인 이름이나 IP주소의 등록자 정보를 알 수 있다. 그렇지만 whois 서버가 외국계이기 때문에 KR도메인 정보는 얻지 못하고 국제 도메인 등록 정보만 얻을 수 있다. KR도메인 정보는 KRNIC의 whois 서버를 이용해야 한다.
- ◆ **whois 명령어를 쓸 때는**
www.hosting.kr이라고 입력하면 등록정보를 찾지 못한다. 제외하고 사용하기 바랍니다.



네트워크 관리

- **tcpdump**

- ◆ tcpdump는 패킷 모니터링을 위한 트래픽 덤프 툴입니다.

- ◆ **192.128.1.1 host로 오고가는 또는 제외한 트래픽**

- ❖ tcpdump host 192.128.1.1
 - ❖ tcpdump 192.128.1.1
 - ❖ tcpdump 192.128.1.1
 - ❖ tcpdump 192.128.1.1



네트워크 관리

- 예)

- ◆ 192.128.1.1과 192.128.1.2 사이를 오고가는 트래픽만

- ❖ tcpdump host 192.128.1.1 and 192.128.1.2

- ◆ ICMP, ARP, UDP 프로토콜만, ICMP 프로토콜 20개만

- ❖ tcpdump icmp -i eth0

- ❖ tcpdump arp

- ❖ tcpdump udp

- ❖ tcpdump icmp -c 20

- ◆ 웹 포트로 오고가는 패킷만

- ❖ tcpdump port 80



네트워크 관리

- fuser

- ◆ 파일이나 소켓을 사용하는 프로세스 ID를 보여줌

- ◆ TCP 25(mail)포트를 사용하는 PID를 보여줌

- # fuser -n tcp 25

- mail/tcp: 3687

- ◆ http 포트를 사용하는 PID, USER, 명령어를 보여줌(-vn을 -nv 처럼 사용해서는 안됨)

- # fuser -vn

```
root@study: ~  
root@study:~# fuser -vn tcp http  
http/tcp:      USER      PID ACCESS COMMAND  
               root       1759 F.... apache2  
               www-data   3075 F.... apache2  
               www-data   3076 F.... apache2  
               www-data   3077 F.... apache2  
               www-data   3078 F.... apache2  
               www-data   3079 F.... apache2  
root@study:~#
```




네트워크 관리

● socket

- ◆ TCP/IP로 통신을 행하는 컴퓨터가 가지는 네트워크 내에서의 주소에 해당하는 IP어드레스와, IP 어드레스의 서브(보조)어드레스인 포트 번호를 조합한 네트워크 어드레스를 말한다.
- ◆ 보통 TCP/IP통신에 있어서는 하나의 IP어드레스는 여러(보통은 65536개)개의 [포트]로 구성되며, 다른 IP어드레스 상의 포트와 결합하여 여러 어드레스와 동시에 통신 가능 하도록 되어 있다. 접속을 할 경우에는 반드시 IP어드레스와 포트 번호의 짝을 지정하며, 이 짝을 소켓이라고 한다.
- ◆ /etc/protocols 파일에 지원하는 프로토콜 정보가 정의되어 있다.



네트워크 관리

• port

- ◆ 포트는 tcp, udp 가 작동하는 전송계층에서 상위 계층의 어플리케이션을 구별하기 위한 일종의 서비스 구분 번호입니다. 그건 tcp 나 udp 헤더에 송신지 포트와 수신지 포트가 들어있다.
- ◆ /etc/services 파일에 각 서비스의 포트번호가 정되어 있다.

• 포트와 소켓 개념도

