



# Networking in Linux





Chonnam National University  
School of Electronics and Computer  
Engineering

Kyungbaek Kim

# Remote Access to Linux

- Remote Access
  - Text based 
  - Window based
- Using applications and protocols based on IP network
  - telnet, ssh
  - xrdp
- Connection Privileges
  - Guest : logins are not required 
  - Full : requires username and password

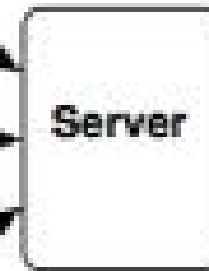
# Before using the applications

- We need to know the basic concept of IP networking
  - Client/Server 
  - Hostname/Domain 
  - IP address 
  - Network Interface
  - Port 
  - Session

# Client / Server

*Network*

Programs or services  
accessing remote  
services on other  
computer system  
through networks



*msg*

*msg*

*msg*



Server computers  
or server programs  
providing various  
services to clients  
through networks

Connect to  
altair.chonnam.ac.kr:23



hostname.domainname  
(altair.chonnam.ac.kr)

IP address  
(168.131.33.33)

Port  
(23 → telnet)

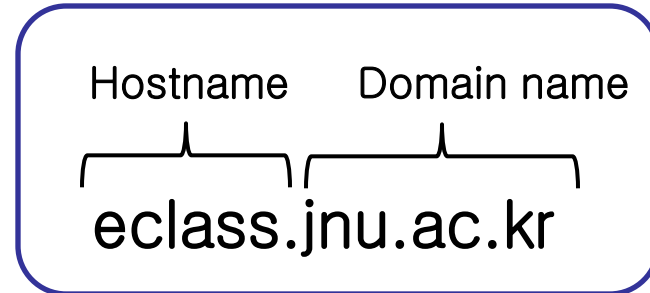
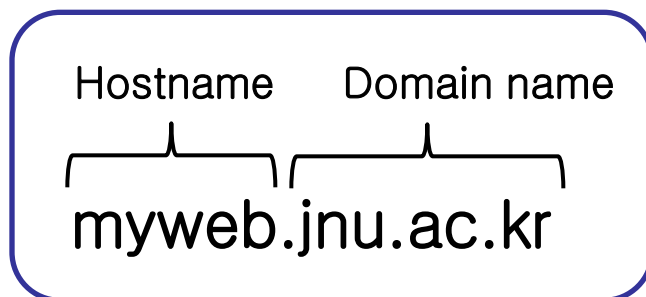
Same

Meaning

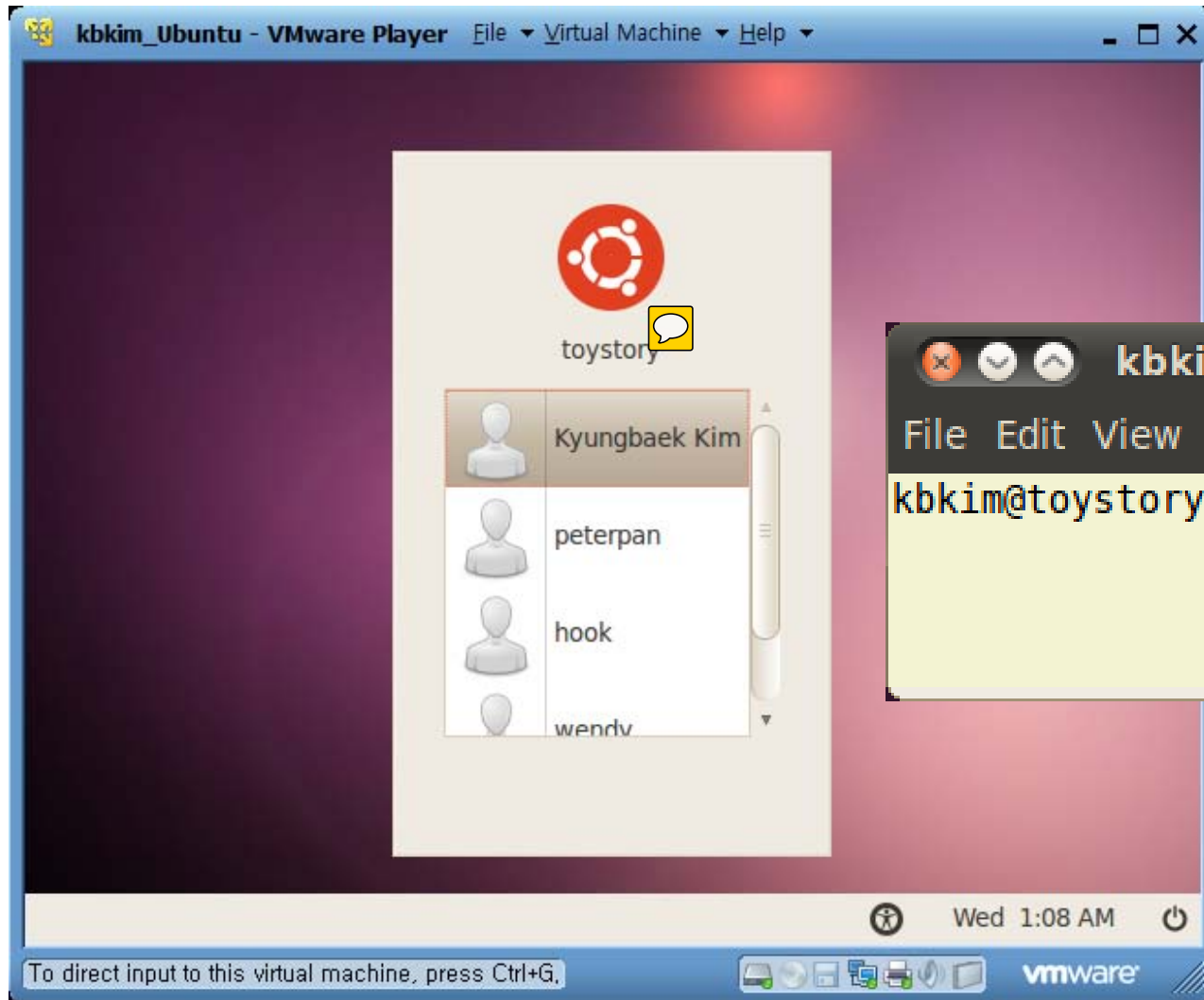
Connect to  
168.131.33.33:23

# Host name and Domain name



- Host name
  - The name of the system
  - Returned by “gethostname” function or “hostname” command
- Domain name
  - The NIS domain name of the system
  - Group the hosts into a domain
  - NIS : Network Information System
    - i.e.) Network naming system



# Example of hostname



# How to set hostname


- `$ hostname <new_host_name>`
  - Set hostname as “new\_host\_name”
  - **Temporally**  set the hostname
  - After rebooting, the hostname sets back to the old host name
- Edit “/etc/hosts”  file and “/etc/hostname” file
  - **Permanently** change the hostname

# Example of changing hostname

```
kbkim@toystory: /etc
File Edit View Terminal Help
kbkim@toystory:/etc$ cat hosts
127.0.0.1    localhost
127.0.1.1    toystory

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
kbkim@toystory:/etc$ cat hostname
toystory
kbkim@toystory:/etc$ hostname
toystory
kbkim@toystory:/etc$ hostname test
hostname: you must be root to change the host name
kbkim@toystory:/etc$ sudo hostname test
[sudo] password for kbkim:
kbkim@toystory:/etc$
```

After changing  
hostname, start  
a new terminal

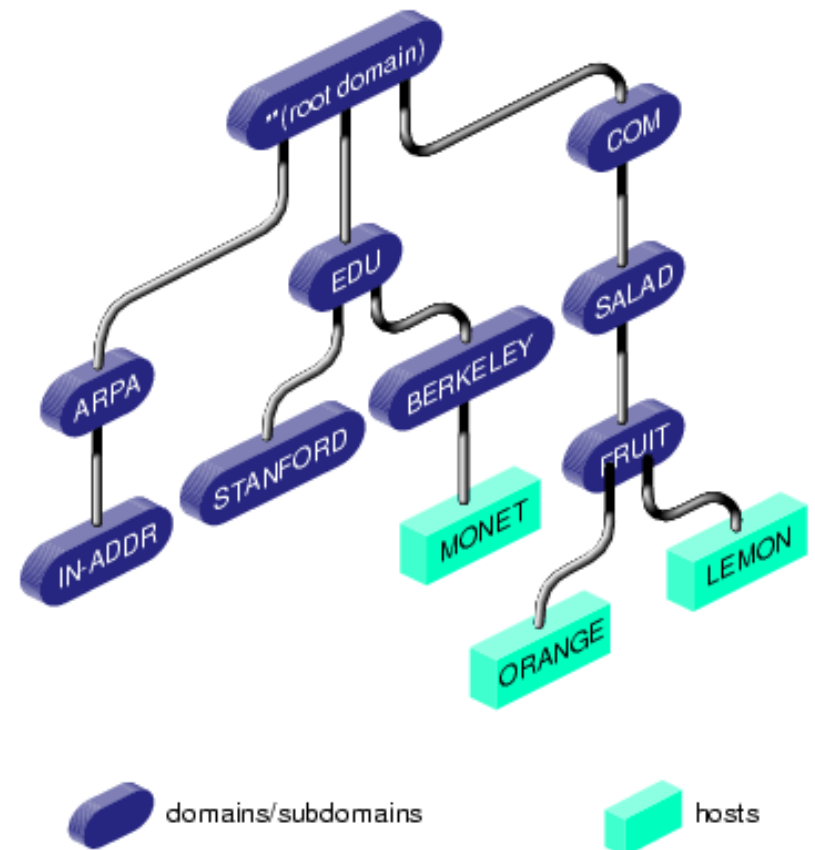
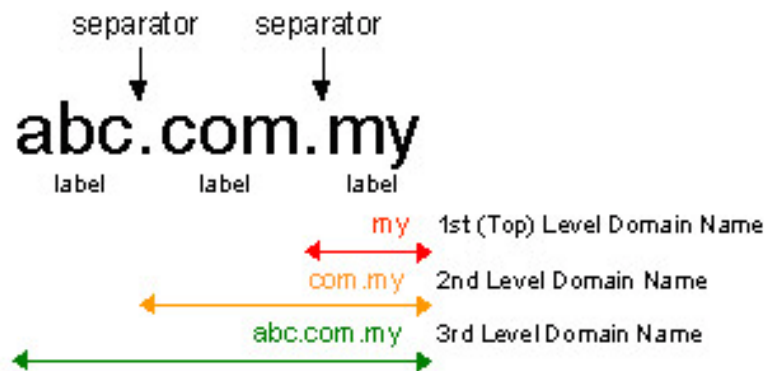


```
kbkim@test: ~
File Edit View Terminal Help
kbkim@test:~$
```




# Domain name

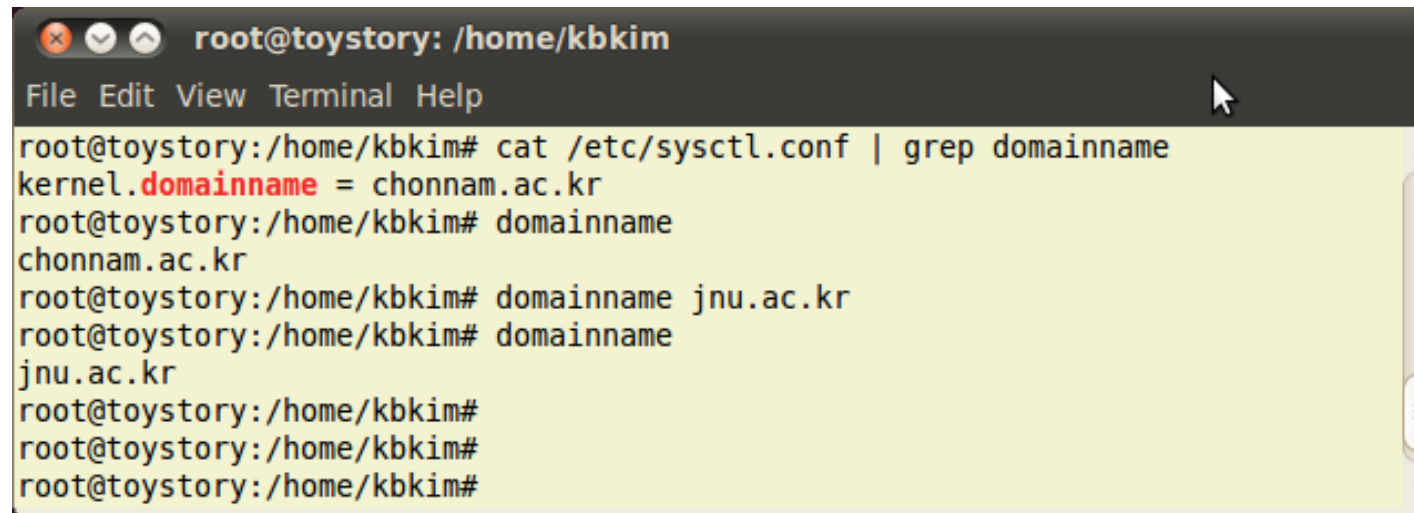
- Domain name is managed by multiple levels
  - Grouping purpose
  - Better management



# How to set domain name

- \$ domain <new\_domain\_name>
  - Set domain name as “new\_domain\_name”
  - **Temporarily**  set the domain name
  - After rebooting, the domain name set back to the old domain name
- Edit “/etc/sysctl.conf” file
  - e.g.) kernel.domainname = chonnam.ac.kr
  - **Permanently** change the domainname

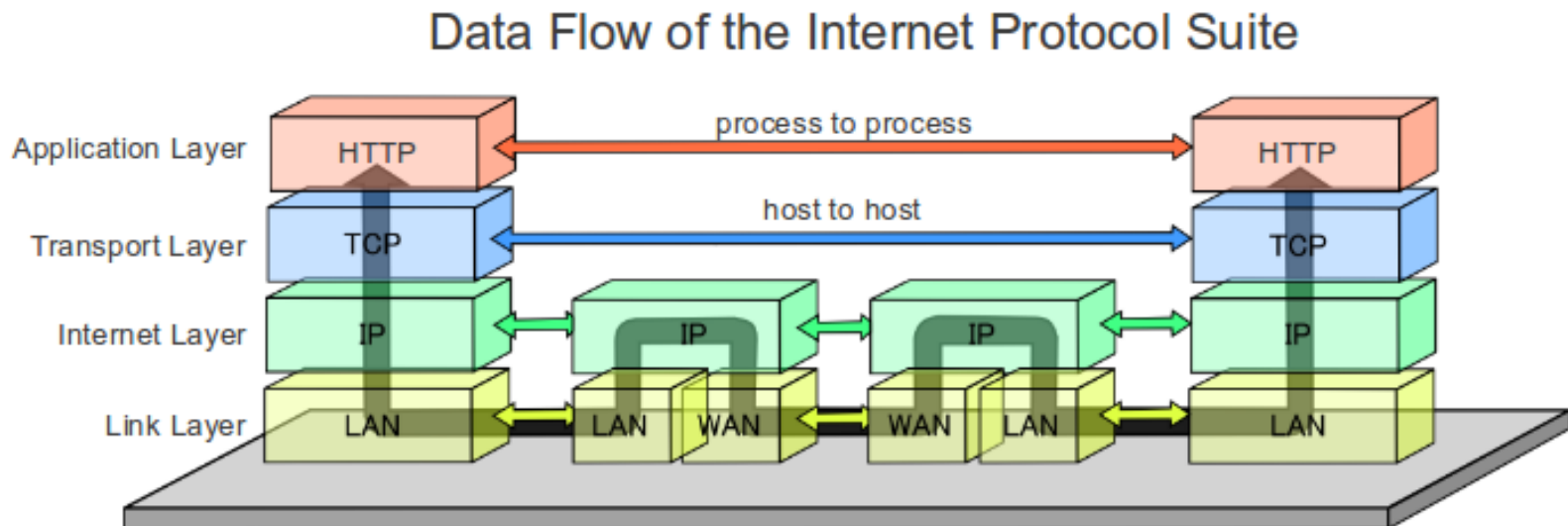
# Example of changing domain name

A terminal window titled 'root@toystory: /home/kbkim' with a menu bar 'File Edit View Terminal Help'. The terminal shows the following commands and output:

```
root@toystory:/home/kbkim# cat /etc/sysctl.conf | grep domainname
kernel.domainname = chonnam.ac.kr
root@toystory:/home/kbkim# domainname
chonnam.ac.kr
root@toystory:/home/kbkim# domainname jnu.ac.kr
root@toystory:/home/kbkim# domainname
jnu.ac.kr
root@toystory:/home/kbkim#
root@toystory:/home/kbkim#
root@toystory:/home/kbkim#
```

# IP addressing

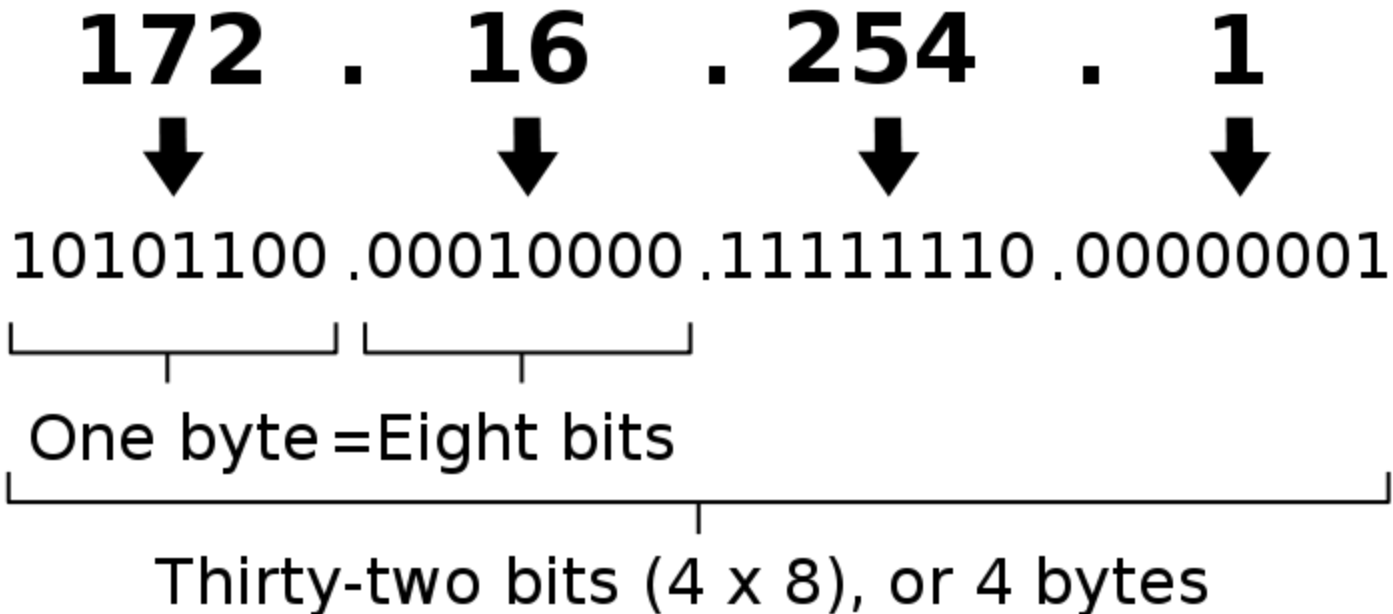
- In these days, computer hosts are addressed by using Internet Protocol (IP) in general.
  - Transport Protocols(TCP/UDP) and Application protocols (HTTP, STP, SOAP..) identify a computer host by using IP address



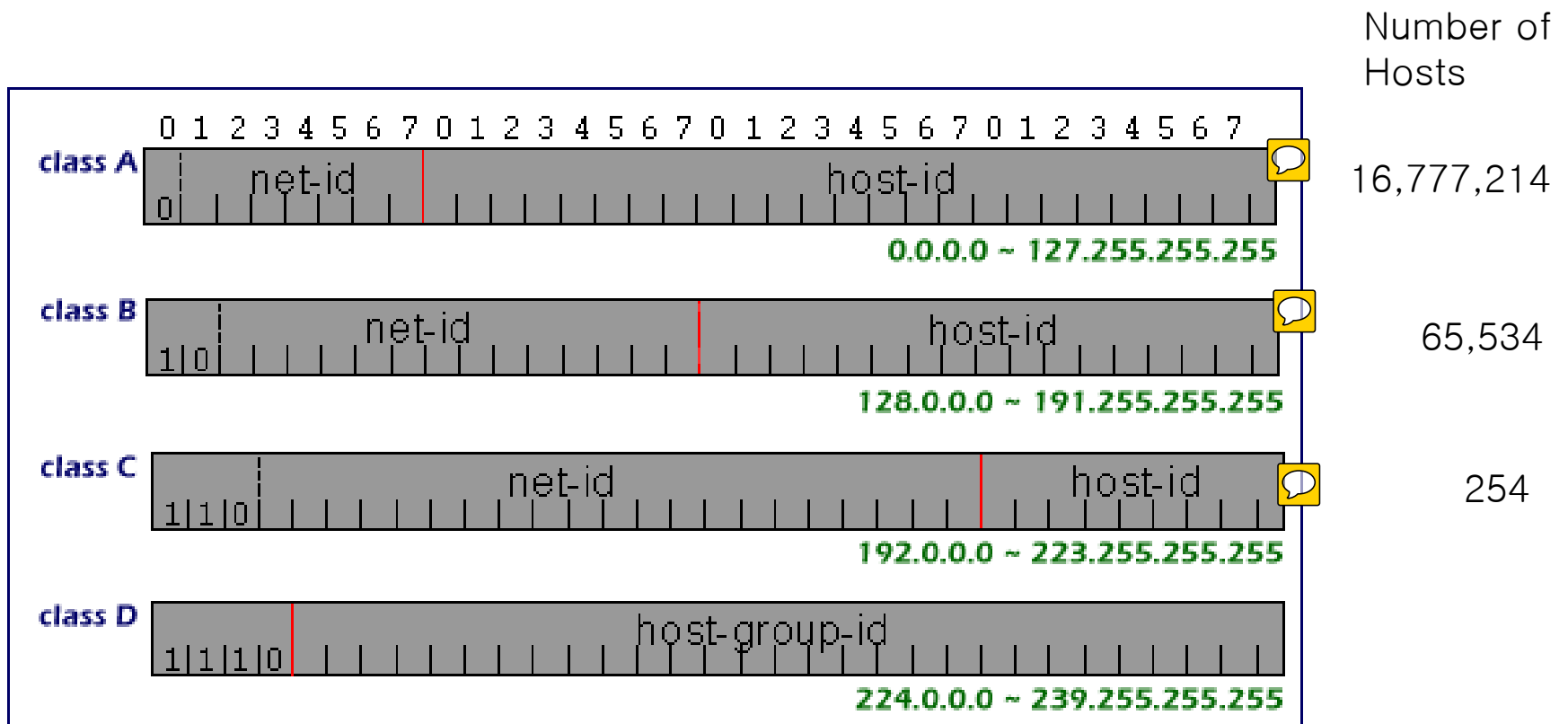
# Anatomy of IPv4 address

- TCP/IP addressing is known as IPv4 addressing
  - Internet Protocol version 4 : 32 bits
    - c.f.) IPv6 is for future needs : 128 bits

An IPv4 address (dotted-decimal notation)





# IPv4 address class ranges





Internet Assigned Numbers Authority (IANA) manages the IP address space allocation

# Subnetting

- Class A and B  may have sub-network.
  - Since host ID portion is very big
- Subnets can be helpful for separating workgroups within a big organizations
  - e.g.) subnet : 128.10.\*.\* (“\*” means any value)
    - ➔ range : 128.10.0.0 ~ 128.10.255.255
- Example
  - 128.10.10.10 and 128.10.200.20 
    - In the same network 128.10.\*.\*
    - But in different sub-networks
      - ➔ 128.10.10.\* and 128.10.200.\*

# Subnet Masks

- Identify which part of an IP address is the network portion
  - That is, Identify which part is the host
- Referred to as “*netmasks*”
  - For class B, default Netmasks → 255.255.0.0 
  - For class C, default Netmasks → 255.255.255.0 
  - For a subnet whose range is between 192.168.10.128 and 192.168.10.255  
→ 255.255.255.128 (\*.\*.\*.10000000)
  - For a subnet whose range is between 192.168.1.192 and 192.168.1.255  
→ 255.255.255.192 (\*.\*.\*.11000000)



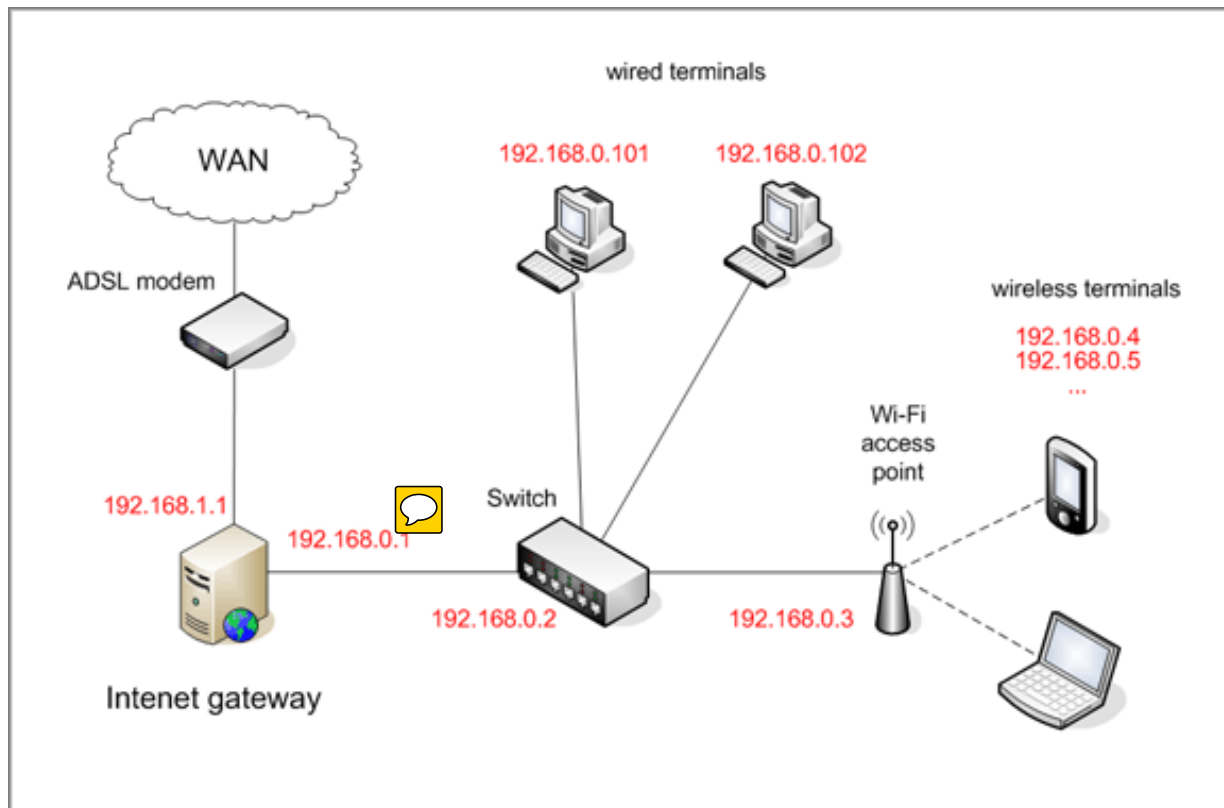
# CIDR notation

- Specify how many bits of IPv4 address are used for subnet portion.
  - /8 : 8 bits are used for subnet mask, Class A
  - /16 : 16 bits are used for subnet mask, Class B


CIDR notation	<u>Netmask notation</u>	$2^{(32-n)}$	Available hosts	Note
/0	0.0.0.0	4,294,967,296	4,294,967,294	The whole Internet
/8	255.0.0.0	16,777,216	16,777,214	Class A
/16	255.255.0.0	65,535	65,533	Class B
/24	255.255.255.0	256	254	Class C
/25	255.255.255.128	128	126	
/26	255.255.255.192	64	62	
/27	255.255.255.224	32	30	
/28	255.255.255.240	16	14	
/29	255.255.255.248	8	6	
/30	255.255.255.252	4	2	
/31	255.255.255.254	2	2*	
/32	255.255.255.255	0	1*	

# Gateway

- A point (IP address) to forward data to Internet



# How to obtain IP addresses


- A machine may have multiple IP addresses 
  - Based on the number of network interfaces
  - A machine with “n” network interfaces can obtain “n” different IP addresses
- That is, **a network interface obtains an IP address**
  - Designated IP address
  - Dynamic IP address
    - DHCP : Dynamic Host Configuration Protocol

# What is a network interface

- Network device for communicating with other machine (interface)
  - Wired LAN card
  - Wireless LAN card
  - Loopback device
- Representation
  - `eth*` : `eth0`, `eth1`, ...
  - `lo` : loopback



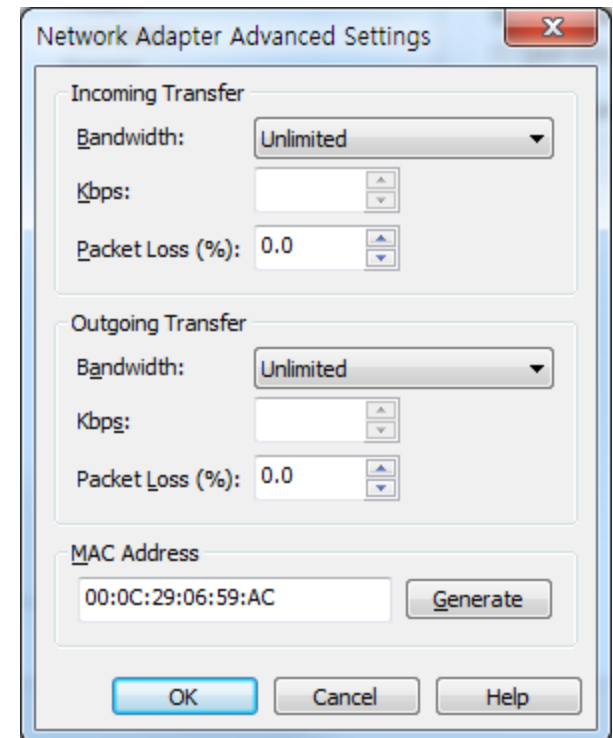
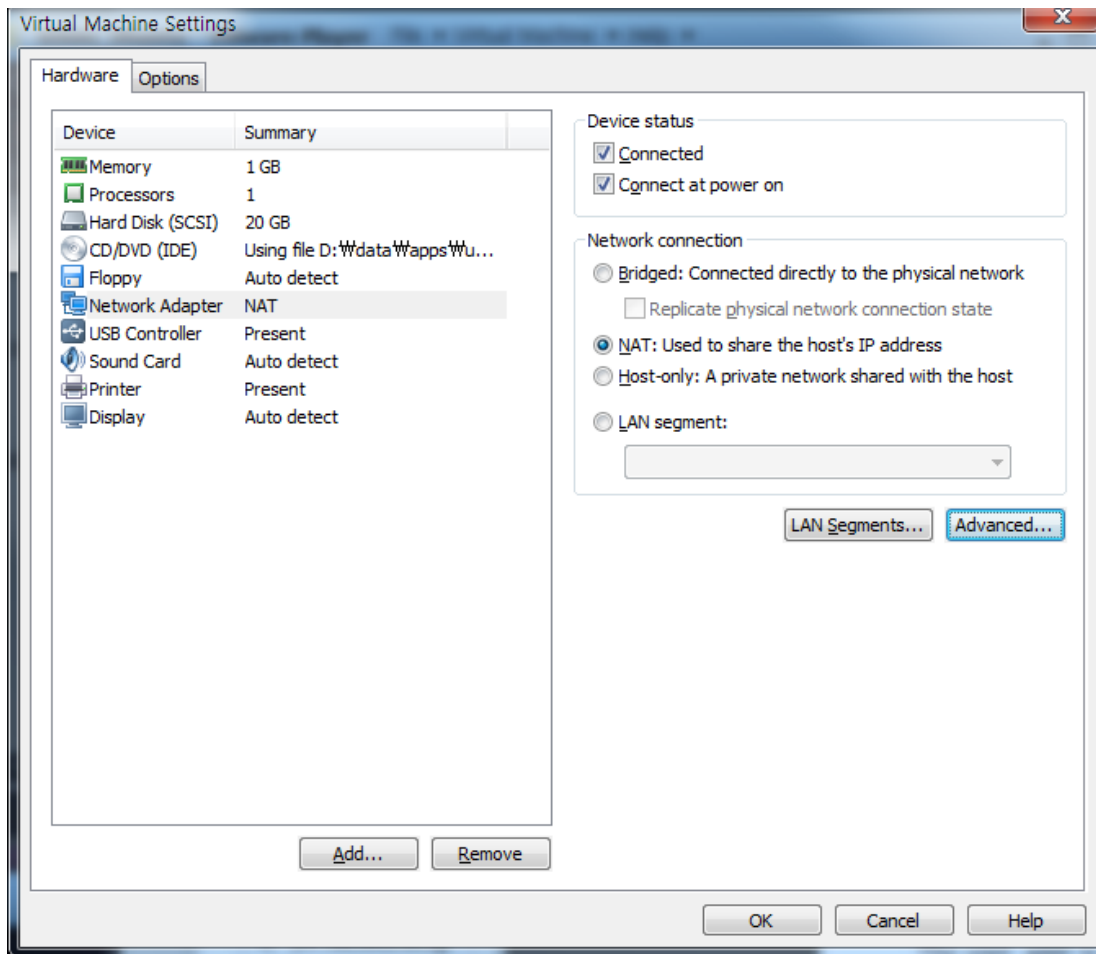
# Network Interface Cards (NIC)

- A computer must have a network interface card to connect to a network
- Each NIC has a unique address
  - The hardware address, known as **MAC address**  (Media access control)
  - e.g. 00:60:08:8F:5A:D9
- MAC address is used by DHCP (Dynamic Host Configuration Protocol) to identify a specific host
- Also used by the ARP (Address Resolution Protocol)
  - To map hosts to IP addresses

# Virtual Network Interfaces

- Sometimes you need a network interface which emulates a network interface card
  - e.g. NIC of VMWare
- VMWare virtually create a network interface card and assign a network interface

# Example



# Configure the network interfaces



- “ifconfig” command
  - Configure the kernel-resident network interfaces
  - Activate or Deactivate NIC
  - Change linux machine’s IP address, netmask, or broadcast address
  - Create an IP alias to allow more than one IP address on your NIC
  - Set a destination address for a point to point connection



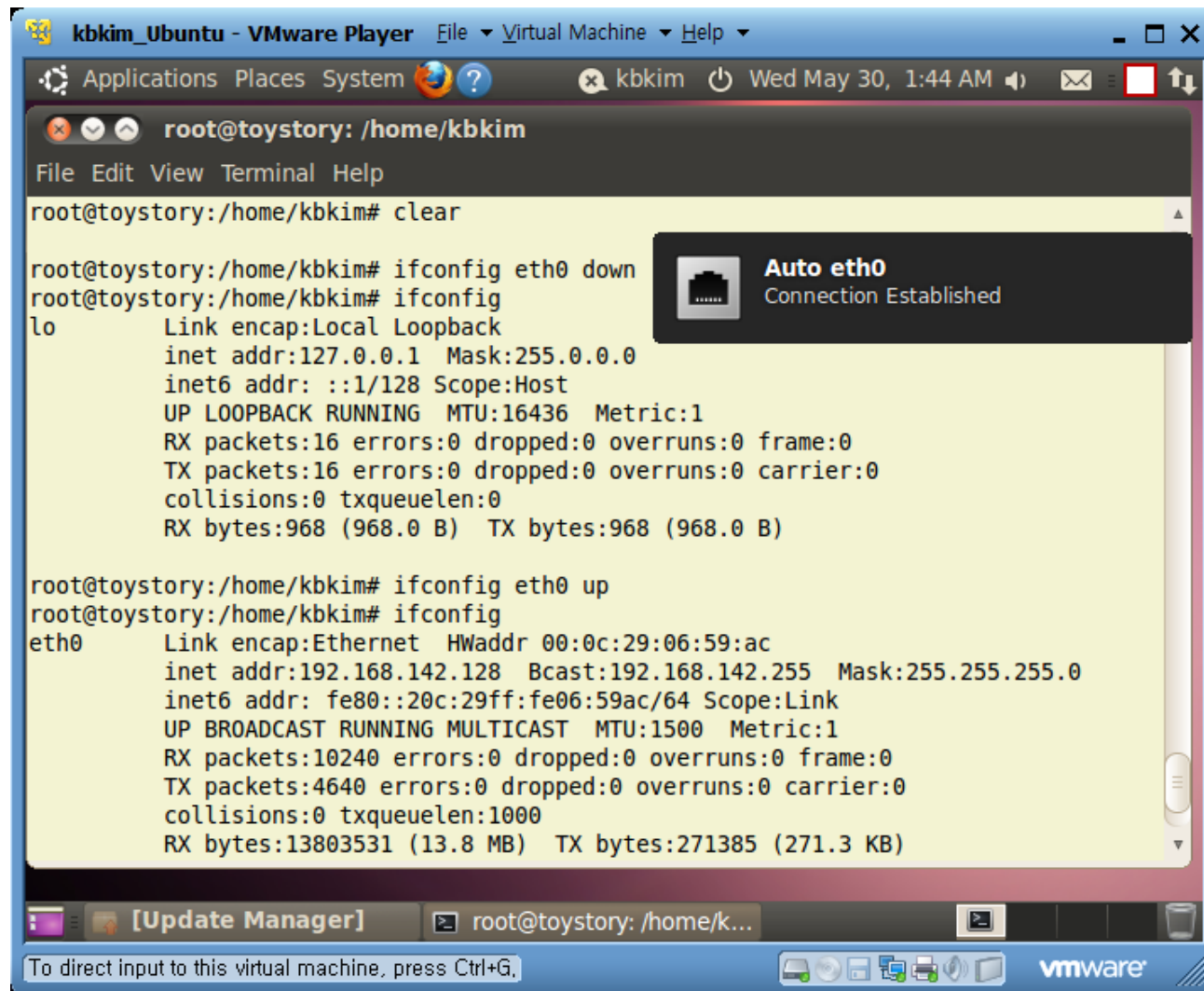
# Checking the status of network interfaces – “ifconfig”

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ ifconfig  
eth0: Link encap:Ethernet HWaddr 00:0c:29:06:59:ac  
      inet addr:192.168.142.128 Bcast:192.168.142.255 Mask:255.255.255.0  
      inet6 addr: fe80::20c:29ff:fe06:59ac/64 Scope:Link  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:10217 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:4579 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:13800690 (13.8 MB) TX bytes:262188 (262.1 KB)  
      Interrupt:19 Base address:0x2024  
  
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:12 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:12 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:0  
      RX bytes:720 (720.0 B) TX bytes:720 (720.0 B)  
  
kbkim@toystory:~$
```

# ifconfig Options

Use	Option	Example
Create alias	[network device]	<code>ifconfig eth0:0:[number]</code> 
Change IP address		<code>ifconfig eth0 10.10.10.12</code> 
Change the netmask	<code>netmask [netmask]</code>	<code>fconfig eth0 netmask 255.255.255.0</code>
Change the broadcast	<code>broadcast [address]</code>	<code>ifconfig eth0 broadcast 10.10.10.255</code>
Take interface down	<code>down</code>	<code>ifconfig eth0 down</code>
Bring interface up	<code>up (add IP address)</code>	<code>ifconfig eth0 up (ifconfig eth0 10.10.10.10)</code>

# Example – up and down NIC



```
kbkim_Ubuntu - VMware Player  File  Virtual Machine  Help    
Applications  Places  System  kbkim  Wed May 30, 1:44 AM    
root@toystory: /home/kbkim    
File Edit View Terminal Help    
root@toystory:/home/kbkim# clear    
root@toystory:/home/kbkim# ifconfig eth0 down    
root@toystory:/home/kbkim# ifconfig    
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:16 errors:0 dropped:0 overruns:0 frame:0    
            TX packets:16 errors:0 dropped:0 overruns:0 carrier:0    
            collisions:0 txqueuelen:0    
            RX bytes:968 (968.0 B)  TX bytes:968 (968.0 B)    
root@toystory:/home/kbkim# ifconfig eth0 up    
root@toystory:/home/kbkim# ifconfig    
eth0       Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac    
            inet addr:192.168.142.128  Bcast:192.168.142.255  Mask:255.255.255.0    
            inet6 addr: fe80::20c:29ff:fe06:59ac/64 Scope:Link    
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1    
            RX packets:10240 errors:0 dropped:0 overruns:0 frame:0    
            TX packets:4640 errors:0 dropped:0 overruns:0 carrier:0    
            collisions:0 txqueuelen:1000    
            RX bytes:13803531 (13.8 MB)  TX bytes:271385 (271.3 KB)    
[Update Manager]  root@toystory: /home/k...    
To direct input to this virtual machine, press Ctrl+G.  vmware
```

# Example – Creating virtual interface by aliasing

```
root@toystory: /sys/class/net
File Edit View Terminal Help

root@toystory:/sys/class/net# ping 192.168.142.150
PING 192.168.142.150 (192.168.142.150) 56(84) bytes of data.
From 192.168.142.128 icmp_seq=1 Destination Host Unreachable
From 192.168.142.128 icmp_seq=2 Destination Host Unreachable
From 192.168.142.128 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.142.150 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3017ms
, pipe 3
root@toystory:/sys/class/net# ifconfig eth0:0 192.168.142.150 netmask 255.255.255.0
root@toystory:/sys/class/net# ping 192.168.142.150
PING 192.168.142.150 (192.168.142.150) 56(84) bytes of data.
64 bytes from 192.168.142.150: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 192.168.142.150: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 192.168.142.150: icmp_seq=3 ttl=64 time=0.026 ms
^C
--- 192.168.142.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.024/0.026/0.029/0.004 ms
root@toystory:/sys/class/net# ifconfig | grep eth0:0
eth0:0      Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
root@toystory:/sys/class/net# ifconfig | grep eth0
eth0        Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
eth0:0      Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
root@toystory:/sys/class/net# ifconfig eth0:0 down
root@toystory:/sys/class/net#
```

# Available Network Interfaces

- To figure out the available network interfaces
- “lshw” command
  - e.g. `lshw -class network`
- “/sys/class/net” directory

# Example


```
root@toystory: /sys/class/net
File Edit View Terminal Help

root@toystory:/sys/class/net# ls -l
total 0
lrwxrwxrwx 1 root root 0 2012-05-30 01:22 eth0 -> ../../devices/pci0000:00/0000:
00:11.0/0000:02:01.0/net/eth0
lrwxrwxrwx 1 root root 0 2012-05-30 01:22 lo -> ../../devices/virtual/net/lo
root@toystory:/sys/class/net# lshw -class network
*-network
    description: Ethernet interface
    product: 79c970 [PCnet32 LANCE]
    vendor: Advanced Micro Devices [AMD]
    physical id: 1
    bus info: pci@0000:02:01.0
    logical name: eth0
    version: 10
    serial: 00:0c:29:06:59:ac
    size: 1GB/s
    capacity: 1GB/s
    width: 32 bits
    clock: 33MHz
    capabilities: bus_master rom ethernet physical logical tp 1000bt-fd
    configuration: autonegotiation=off broadcast=yes driver=vmxnet driververs
ion=2.0.8.0 duplex=full firmware=N/A ip=192.168.142.128 latency=64 link=yes maxl
atency=255 mingnt=6 multicast=yes port=twisted pair speed=1GB/s
    resources: irq:19 ioport:2000(size=128) memory:d8400000-d840ffff(prefetch
able)
root@toystory:/sys/class/net#
```

# Loopback address and interface

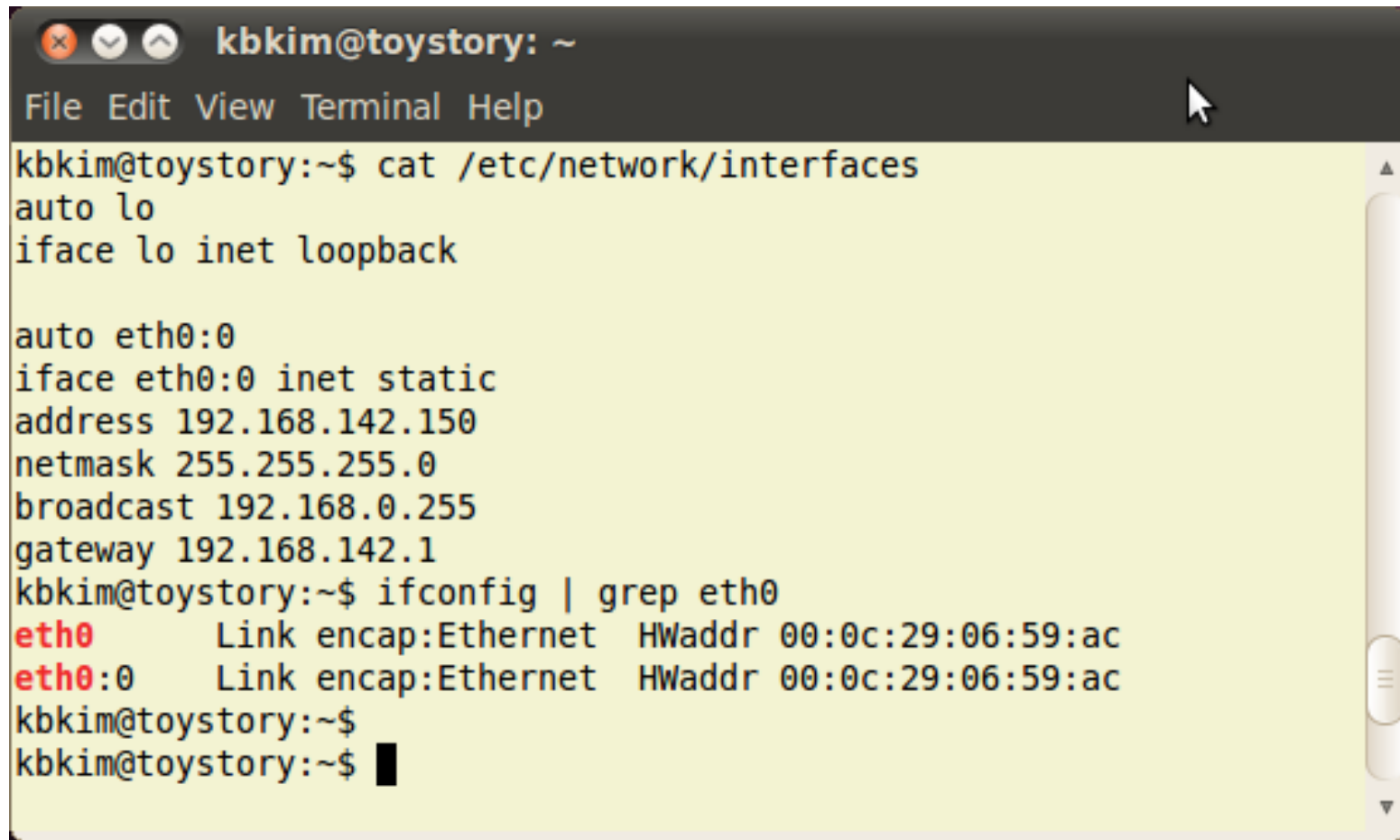


# Permanently setting NIC

- Modify “/etc/network/interfaces” file
  - Network interface configuration for ifup and ifdown commands
  - Line starting with “#” is ignored.
  - Using DHCP
    - iface eth0 inet dhcp
  - Using static setting
    - auto eth0:0 
    - iface eth0:0 inet static
    - address 192.168.142.150
    - netmask 255.255.255.0
    - broadcast 192.168.142.255
    - gateway 192.168.142.1
- “/etc/init.d/networking restart” for restart the network



# Example



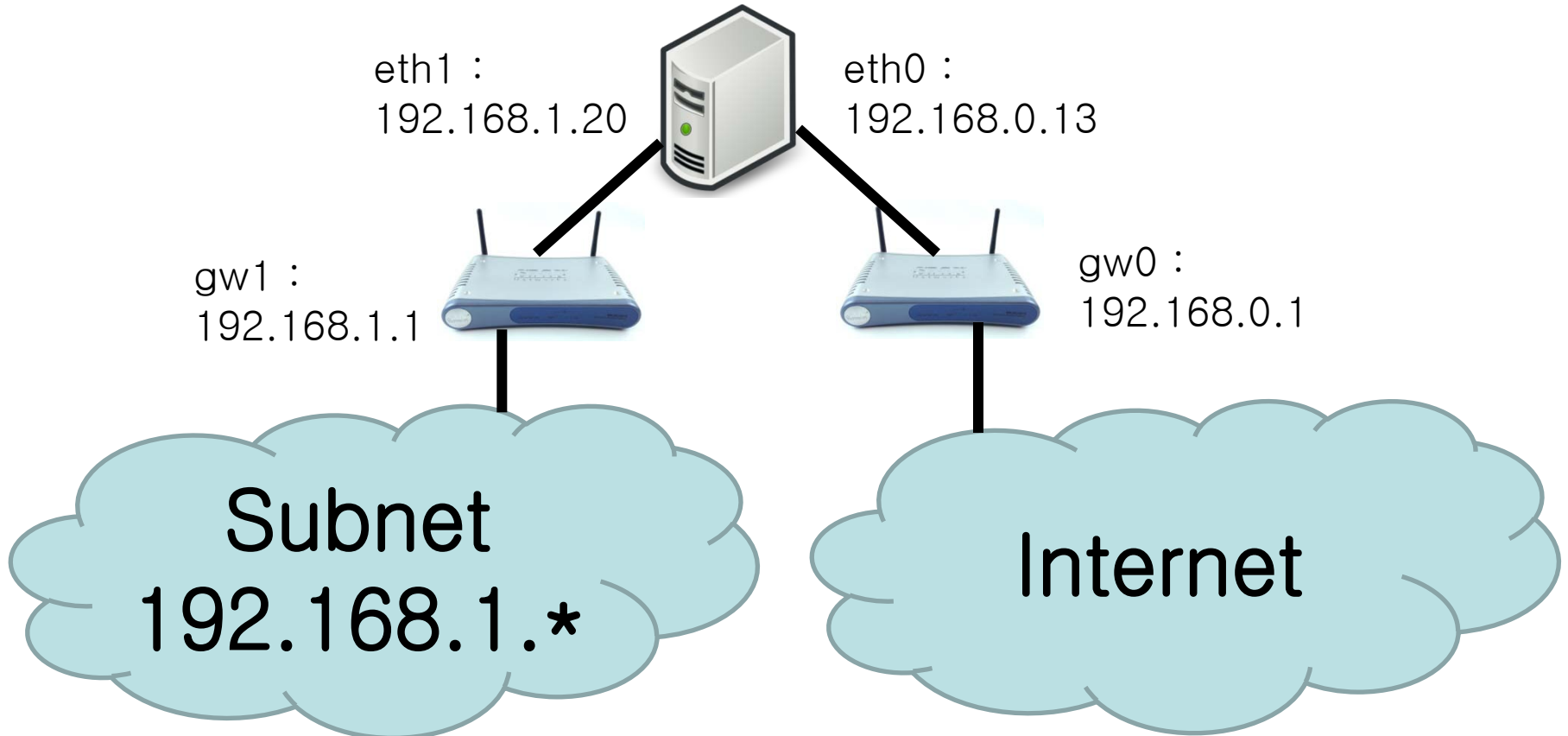
A terminal window titled "kbkim@toystory: ~" with a menu bar containing "File", "Edit", "View", "Terminal", and "Help". The terminal displays the following commands and output:

```
kbkim@toystory:~$ cat /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0:0
iface eth0:0 inet static
address 192.168.142.150
netmask 255.255.255.0
broadcast 192.168.0.255
gateway 192.168.142.1
kbkim@toystory:~$ ifconfig | grep eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
eth0:0    Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
kbkim@toystory:~$
kbkim@toystory:~$
```

# Route setup

- \* Routing : finding a path to reach a destination
  - Which gateway is used to reach a machine with IP 192.168.1.30? → gw1
  - Which gateway is used to reach a machine with IP 169.254.10.15? → gw0
  - Which gateway is used to reach machines in a subnet 192.168.1.\*? → gw1



# Configure Route

- “route” command
  - Builds/shows the routing tables (in memory) implemented for routing packets
  - c.f. “ifconfig” initialized the interface
- Syntax
  - route [commands] [options] target [parameters]
  - “add/del” command → add/delete a target
  - “-n” option → numerical representation
  - “default” option → to set default gateway (no need target)
  - “-net” or “-host” option → target is network or host
  - “gw GW” parameter → gateway GW(IP address)
  - “dev if” parameter → interface (e.g. eth0)

# Example

```
root@toystory: /home/kbkim
File Edit View Terminal Help

root@toystory:/home/kbkim# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.142.0    *                255.255.255.0    U        1      0      0 eth0
link-local       *                255.255.0.0      U       1000    0      0 eth0
default          192.168.142.2    0.0.0.0          UG        0      0      0 eth0
root@toystory:/home/kbkim# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.142.0    0.0.0.0          255.255.255.0    U        1      0      0 eth0
169.254.0.0      0.0.0.0          255.255.0.0      U       1000    0      0 eth0
0.0.0.0          192.168.142.2    0.0.0.0          UG        0      0      0 eth0
root@toystory:/home/kbkim# route add default gw 192.168.142.3
root@toystory:/home/kbkim# route add -net 192.168.113.0 netmask 255.255.255.0 gw 192.168.142.5
root@toystory:/home/kbkim# route add -net 192.168.114.0 netmask 255.255.255.0 gw 192.168.142.6
root@toystory:/home/kbkim# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.113.0    192.168.142.5    255.255.255.0    UG        0      0      0 eth0
192.168.114.0    192.168.142.6    255.255.255.0    UG        0      0      0 eth0
192.168.142.0    0.0.0.0          255.255.255.0    U        1      0      0 eth0
169.254.0.0      0.0.0.0          255.255.0.0      U       1000    0      0 eth0
0.0.0.0          192.168.142.3    0.0.0.0          UG        0      0      0 eth0
0.0.0.0          192.168.142.2    0.0.0.0          UG        0      0      0 eth0
root@toystory:/home/kbkim# 3~
```

# Example of deletion

```
root@toystory: /home/kbkim
File Edit View Terminal Help

root@toystory:/home/kbkim# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.113.0    192.168.142.5   255.255.255.0    UG      0      0      0 eth0
192.168.114.0    192.168.142.6   255.255.255.0    UG      0      0      0 eth0
192.168.142.0    0.0.0.0          255.255.255.0    U        1      0      0 eth0
169.254.0.0      0.0.0.0          255.255.0.0      U       1000    0      0 eth0
0.0.0.0          192.168.142.3   0.0.0.0          UG      0      0      0 eth0
0.0.0.0          192.168.142.2   0.0.0.0          UG      0      0      0 eth0
root@toystory:/home/kbkim# route del default gw 192.168.142.3
root@toystory:/home/kbkim# route del -net 192.168.113.0 netmask 255.255.255.0 gw 192.168.142.5
root@toystory:/home/kbkim# route del -net 192.168.114.0 netmask 255.255.255.0 gw 192.168.142.6
root@toystory:/home/kbkim# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.142.0    0.0.0.0          255.255.255.0    U        1      0      0 eth0
169.254.0.0      0.0.0.0          255.255.0.0      U       1000    0      0 eth0
0.0.0.0          192.168.142.2   0.0.0.0          UG      0      0      0 eth0
root@toystory:/home/kbkim#
```

# Check the status of network



- “netstat” command
  - Display the status of the network

---

Option	Output
--------	--------

---

-g	Displays the multicast groups configured
----	--

-i	Displays the interfaces configured by ifconfig
----	--

-s	Lists a summary of activity for each protocol
----	---

-v	Gives verbose output, listing both active and inactive sockets
----	--

-c	Updates output every second (good for testing and troubleshooting)
----	--

-e	Gives verbose output for active connections only
----	--

-C	Displays information from the route cache and is good for looking at past connections
----	---

---

# More options of netstat

- “netstat -a” → List all Ports
- “netstat -at” → List all TCP Ports
- “netstat -au” → List all UDP Ports
- “netstat -l” → List all Listen sockets
- “netstat -lt” → List all TCP Listen sockets
- “netstat -lu” → List all UDP Listen sockets
- “netstat -lx” → List all UNIX Listen socket
- “netstat -r” → Display the kernel routing information

# Example of “netstat”

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ netstat -a | more  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost.localdom:3350 *:.*                     LISTEN  
tcp        0      0 localhost.localdoma:ipp *:.*                     LISTEN  
tcp        0      0 *:telnet             *:.*                     LISTEN  
tcp        0      0 *:3389                *:.*                     LISTEN  
tcp6       0      0 localhost:ipp        [::]:.*                 LISTEN  
udp        0      0 *:bootpc             *:.*                     LISTEN  
udp        0      0 *:41038               *:.*                     LISTEN  
udp        0      0 *:mdns                *:.*                     LISTEN  
Active UNIX domain sockets (servers and established)  
Proto RefCnt Flags               Type           State         I-Node      Path  
unix    2      [ ACC ]               STREAM         LISTENING     9019        @/tmp/.ICE-unix/1785  
unix    2      [ ACC ]               STREAM         LISTENING     4113        /var/run/avahi-daemon/socket  
unix    2      [ ACC ]               STREAM         LISTENING     8991        @/tmp/dbus-r9TsVgENn  
unix   17      [ ]                DGRAM          LISTENING     4146        /dev/log  
unix    2      [ ACC ]               STREAM         LISTENING     7159        @/var/run/hald/dbus-fyBR5UdgeZ  
unix    2      [ ACC ]               STREAM         LISTENING     2604        @/com/ubuntu/upstart  
unix    2      [ ACC ]               STREAM         LISTENING     6061        @/tmp/gdm-greeter-ocvazdHh  
unix    2      [ ACC ]               STREAM         LISTENING     7192        @/var/run/hald/dbus-hceKya64A3  
unix    2      [ ACC ]               STREAM         LISTENING     5916        /tmp/.X11-unix/X0  
unix    2      [ ACC ]               STREAM         LISTENING     5915        @/tmp/.X11-unix/X0  
unix    2      [ ACC ]               STREAM         LISTENING     8975        /tmp/ssh-ficSmm1785/agent.1785  
unix    2      [ ACC ]               STREAM         LISTENING     9020        /tmp/.ICE-unix/1785
```



# Example of “netstat”

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ netstat -s | more  
Ip:  
  60 total packets received  
   3 with invalid addresses  
   0 forwarded  
   0 incoming packets discarded  
  57 incoming packets delivered  
  47 requests sent out  
Icmp:  
  1 ICMP messages received  
  0 input ICMP message failed.  
ICMP input histogram:  
  echo requests: 1  
  1 ICMP messages sent  
  0 ICMP messages failed  
ICMP output histogram:  
  echo replies: 1  
IcmpMsg:  
  InType8: 1  
  OutType0: 1  
Tcp:  
  5 active connections openings  
  0 passive connection openings  
  4 failed connection attempts  
  0 connection resets received
```

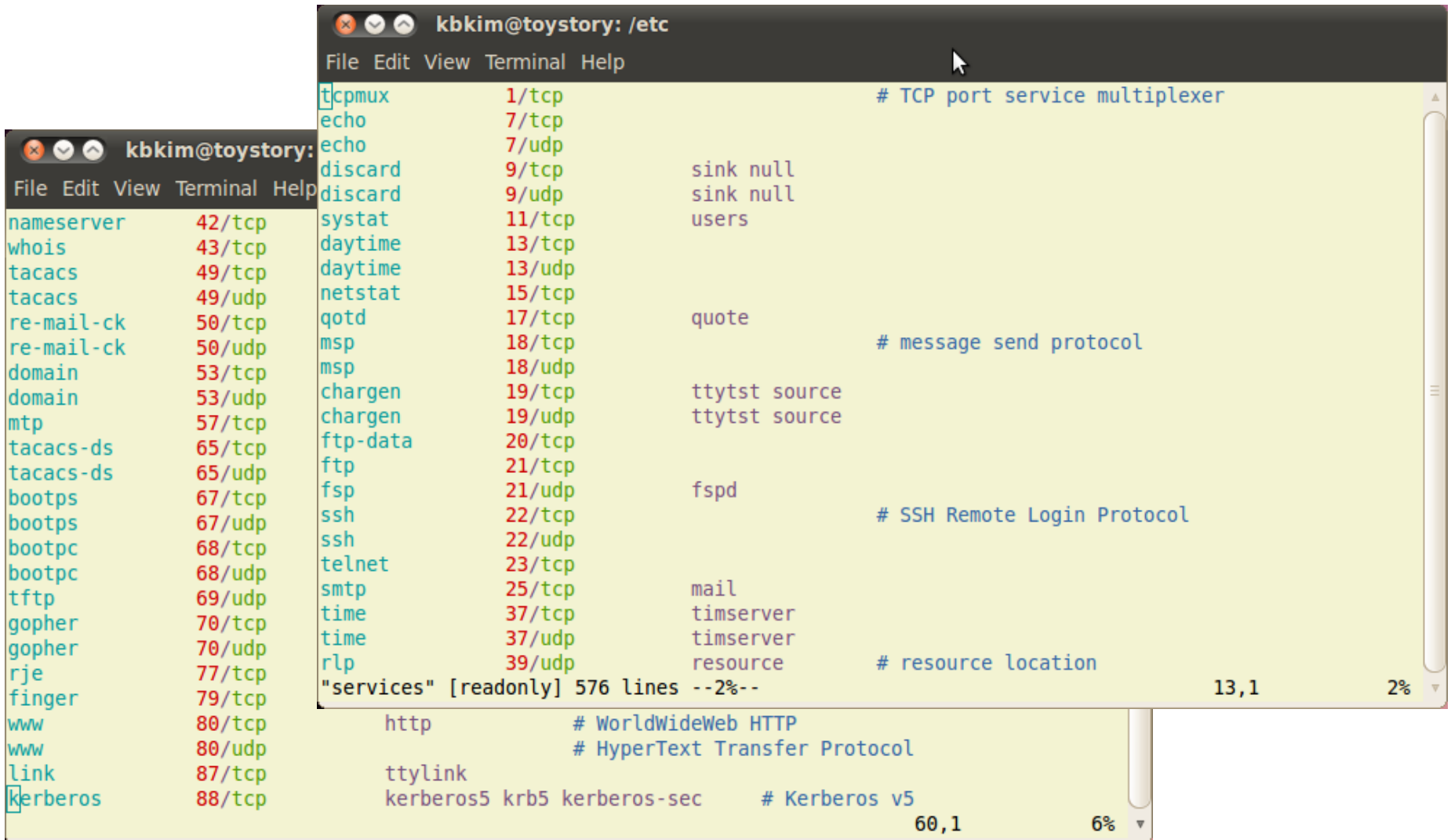
# Example of “netstat”

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ netstat -i  
Kernel Interface table  
Iface    MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg  
eth0      1500 0      52    0      0 0        57    0      0    0 0 BMRU  
lo        16436 0       8    0      0 0         8    0      0    0 0 LRU  
kbkim@toystory:~$ netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp      0      0 localhost.localdom:3350 *:.*                    LISTEN  
tcp      0      0 localhost.localdoma:ipp *:.*                    LISTEN  
tcp      0      0 *:telnet                *:.*                    LISTEN  
tcp      0      0 *:3389                   *:.*                    LISTEN  
tcp6     0      0 localhost:ipp           [::]:.*                 LISTEN  
kbkim@toystory:~$ netstat -r  
Kernel IP routing table  
Destination Gateway      Genmask      Flags   MSS Window  irtt Iface  
192.168.142.0 *            255.255.255.0 U        0 0        0 eth0  
link-local *            255.255.0.0 U        0 0        0 eth0  
default 192.168.142.2 0.0.0.0 UG       0 0        0 eth0  
kbkim@toystory:~$
```

# Port and Services

- IP address → identify a host
- Port → identify a service
  - Used by a socket of TCP or UDP
  - Different services use different ports
  - The information of assigned ports are described in /etc/services file
  - e.g.) ftp : 21/tcp for control  
ftp-data : 20/tcp for data  
www : 80/tcp or 80/udp for http

# /etc/services




```
kbkim@toystory: /etc
File Edit View Terminal Help
tcpmux      1/tcp      # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp      sink null
discard     9/udp      sink null
sysstat     11/tcp      users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp      quote
msp         18/tcp      # message send protocol
msp         18/udp
chargen     19/tcp      ttytst source
chargen     19/udp      ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp      fspd
ssh         22/tcp      # SSH Remote Login Protocol
ssh         22/udp
telnet      23/tcp
smtp        25/tcp      mail
time        37/tcp      timserver
time        37/udp      timserver
rlp         39/udp      resource
# resource location
"services" [readonly] 576 lines --2%--
13,1 2%

kbkim@toystory:
File Edit View Terminal Help
nameserver  42/tcp
whois       43/tcp
tacacs      49/tcp
tacacs      49/udp
re-mail-ck  50/tcp
re-mail-ck  50/udp
domain      53/tcp
domain      53/udp
mtp         57/tcp
tacacs-ds   65/tcp
tacacs-ds   65/udp
bootps      67/tcp
bootps      67/udp
bootpc      68/tcp
bootpc      68/udp
tftp        69/udp
gopher      70/tcp
gopher      70/udp
rje         77/tcp
finger      79/tcp
www         80/tcp
www         80/udp
link        87/tcp
kerberos    88/tcp
http        # WorldWideWeb HTTP
            # HyperText Transfer Protocol
ttyp        ttylink
kerberos5   krb5 kerberos-sec # Kerberos v5
60,1 6%
```

# Popular TCP/UDP ports

Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

# Using DNS

- Translate a hostname to an IP address 
  - In C language : `gethostbyname()` function
- “**nslookup**” command
  - Query Internet name service interactively
- The local name server is set in “`/etc/resolve.conf`” file
  - If using DHCP, this file be set automatically
  - You can set a designated domain name server as well.
    - e.g. Google Public DNS → 8.8.8.8 and 8.8.4.4

# Example

```
kbkim@toystory: /etc
File Edit View Terminal Help

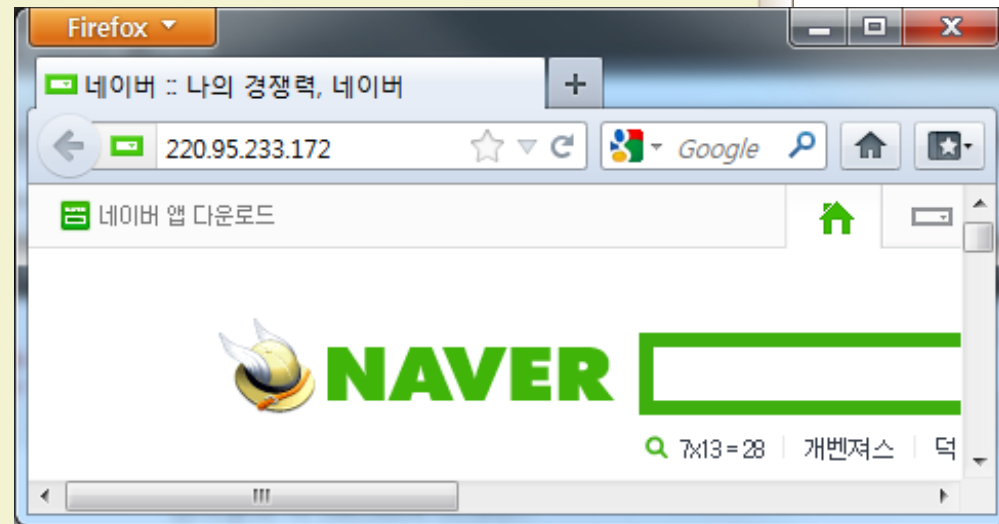
kbkim@toystory:/etc$ cat resolv.conf
# Generated by NetworkManager
domain localdomain
search localdomain
nameserver 192.168.142.2
kbkim@toystory:/etc$ nslookup altair.chonnam.ac.kr
Server:      192.168.142.2
Address:     192.168.142.2#53

Non-authoritative answer:
Name:   altair.chonnam.ac.kr
Address: 168.131.33.33

kbkim@toystory:/etc$ nslookup www.naver.com
Server:      192.168.142.2
Address:     192.168.142.2#53

Non-authoritative answer:
www.naver.com canonical name = www.g.naver.com.
Name:   www.g.naver.com
Address: 202.131.30.11
Name:   www.g.naver.com
Address: 220.95.233.172

kbkim@toystory:/etc$
```



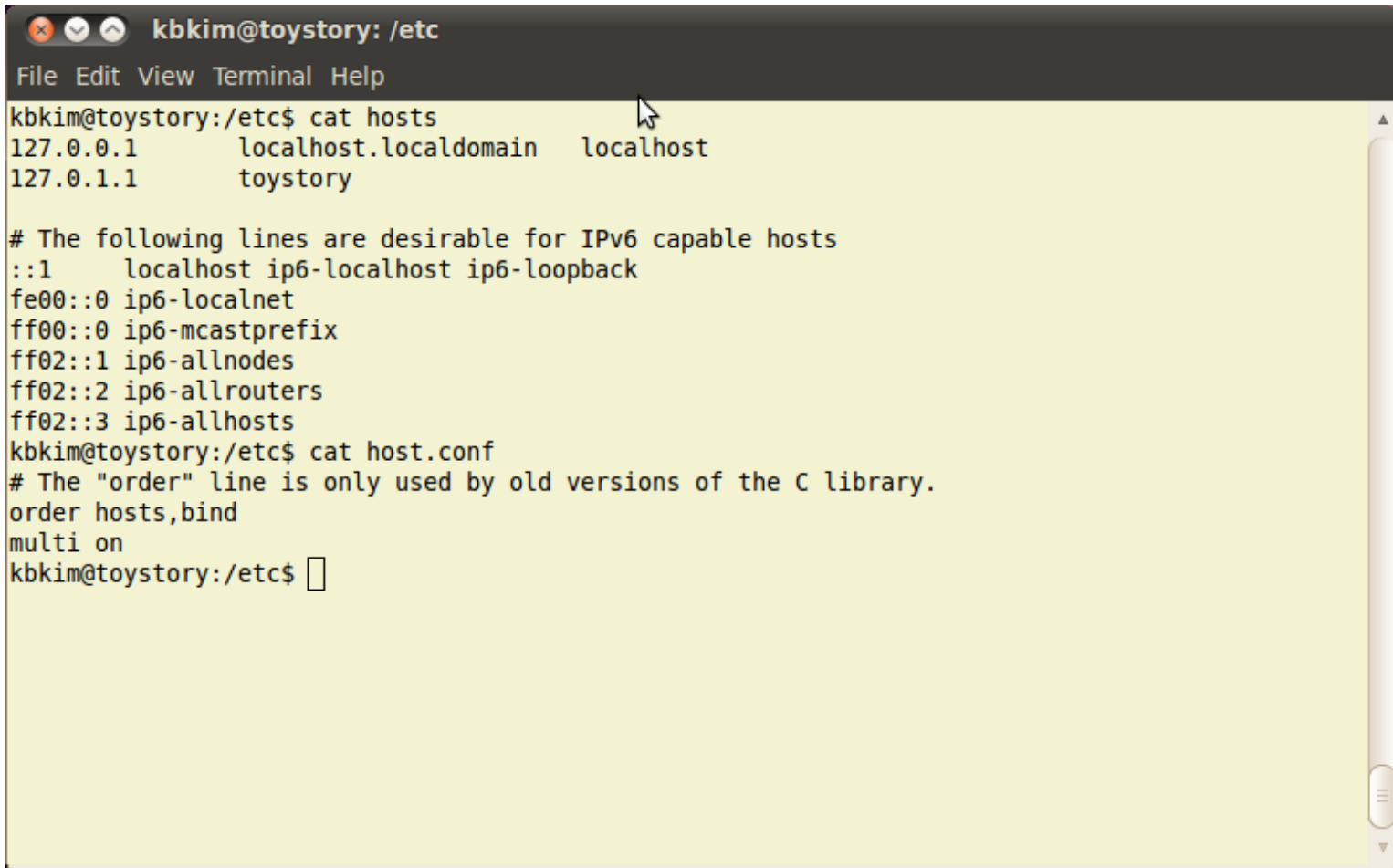
# Local information of hosts



- “/etc/hosts” file contains the information of local hosts
  - A map of IP to hostnames
  - Usually used for managing internal sub networks
- Order of searching a IP address of a hostname
  - Defined in “/etc/host.conf”
  - General order → hosts, then DNS



# Example

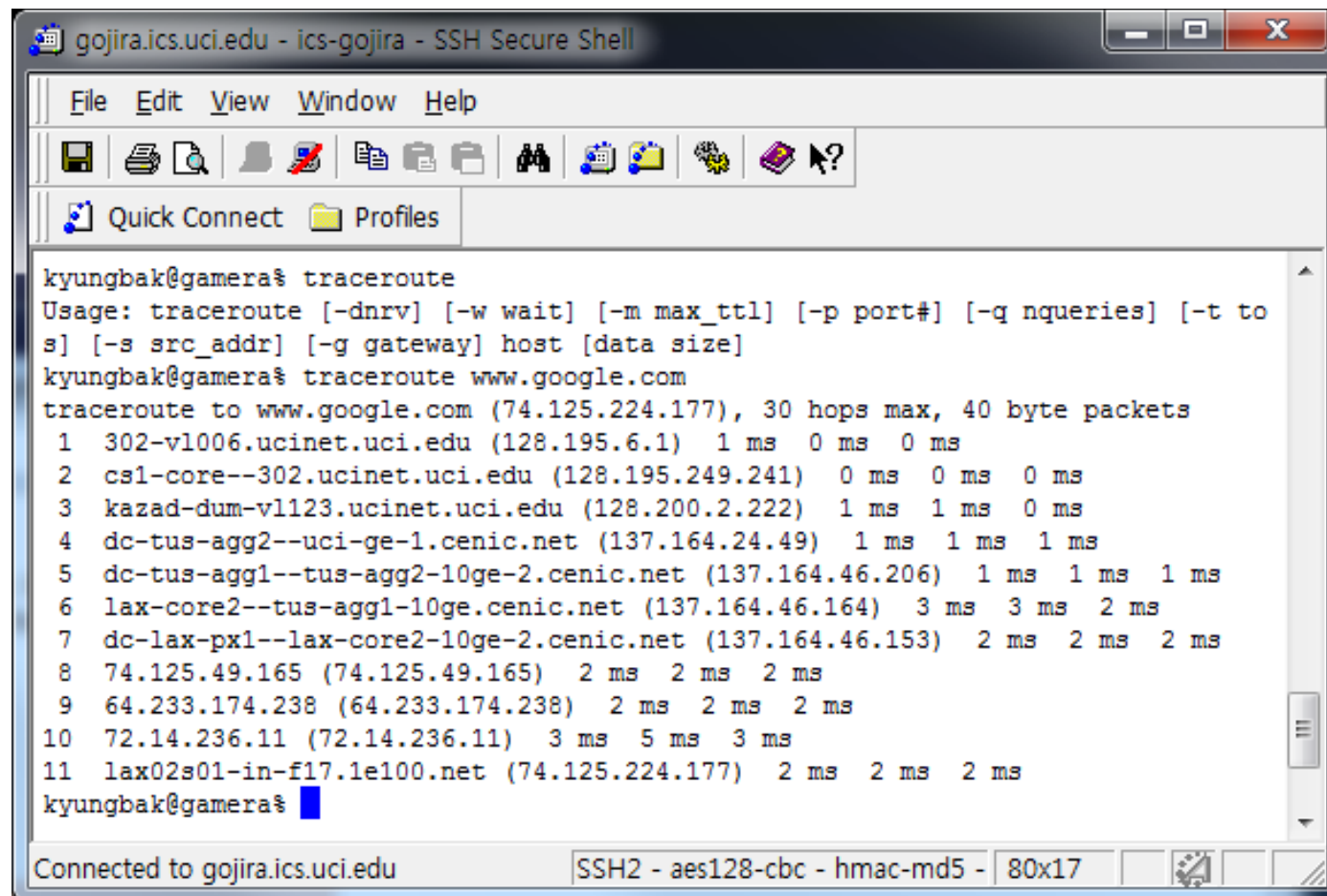
A terminal window titled 'kbkim@toystory: /etc' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the output of 'cat /etc/hosts' and 'cat /etc/host.conf'. The hosts file contains entries for 127.0.0.1, 127.0.1.1, and IPv6 addresses. The host.conf file contains configuration for the C library's gethostbyname function.

```
kbkim@toystory: /etc
File Edit View Terminal Help
kbkim@toystory:/etc$ cat hosts
127.0.0.1      localhost.localdomain  localhost
127.0.1.1      toystory

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
kbkim@toystory:/etc$ cat host.conf
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
kbkim@toystory:/etc$
```

# Check whether IP address/Hostname is reachable

- “traceroute” command



The screenshot shows a terminal window titled "gojira.ics.uci.edu - ics-gojira - SSH Secure Shell". The window has a menu bar (File, Edit, View, Window, Help) and a toolbar with various icons. Below the toolbar, there are tabs for "Quick Connect" and "Profiles". The terminal content shows the user "kyungbak@gamera" running the "traceroute" command. The output displays the path from the user's machine to "www.google.com" (74.125.224.177), showing 11 hops with IP addresses and round-trip times in milliseconds. The status bar at the bottom indicates the connection is to "gojira.ics.uci.edu" using "SSH2 - aes128-cbc - hmac-md5" with a resolution of "80x17".

```
kyungbak@gamera% traceroute
Usage: traceroute [-dnrv] [-w wait] [-m max_ttl] [-p port#] [-q nqueries] [-t to
s] [-s src_addr] [-g gateway] host [data size]
kyungbak@gamera% traceroute www.google.com
traceroute to www.google.com (74.125.224.177), 30 hops max, 40 byte packets
 1  302-vl006.ucinet.uci.edu (128.195.6.1)  1 ms  0 ms  0 ms
 2  cs1-core--302.ucinet.uci.edu (128.195.249.241)  0 ms  0 ms  0 ms
 3  kazad-dum-vl123.ucinet.uci.edu (128.200.2.222)  1 ms  1 ms  0 ms
 4  dc-tus-aggr2--uci-ge-1.cenic.net (137.164.24.49)  1 ms  1 ms  1 ms
 5  dc-tus-aggr1--tus-aggr2-10ge-2.cenic.net (137.164.46.206)  1 ms  1 ms  1 ms
 6  lax-core2--tus-aggr1-10ge.cenic.net (137.164.46.164)  3 ms  3 ms  2 ms
 7  dc-lax-px1--lax-core2-10ge-2.cenic.net (137.164.46.153)  2 ms  2 ms  2 ms
 8  74.125.49.165 (74.125.49.165)  2 ms  2 ms  2 ms
 9  64.233.174.238 (64.233.174.238)  2 ms  2 ms  2 ms
10  72.14.236.11 (72.14.236.11)  3 ms  5 ms  3 ms
11  lax02s01-in-f17.1e100.net (74.125.224.177)  2 ms  2 ms  2 ms
kyungbak@gamera%
```

Connected to gojira.ics.uci.edu      SSH2 - aes128-cbc - hmac-md5 - 80x17

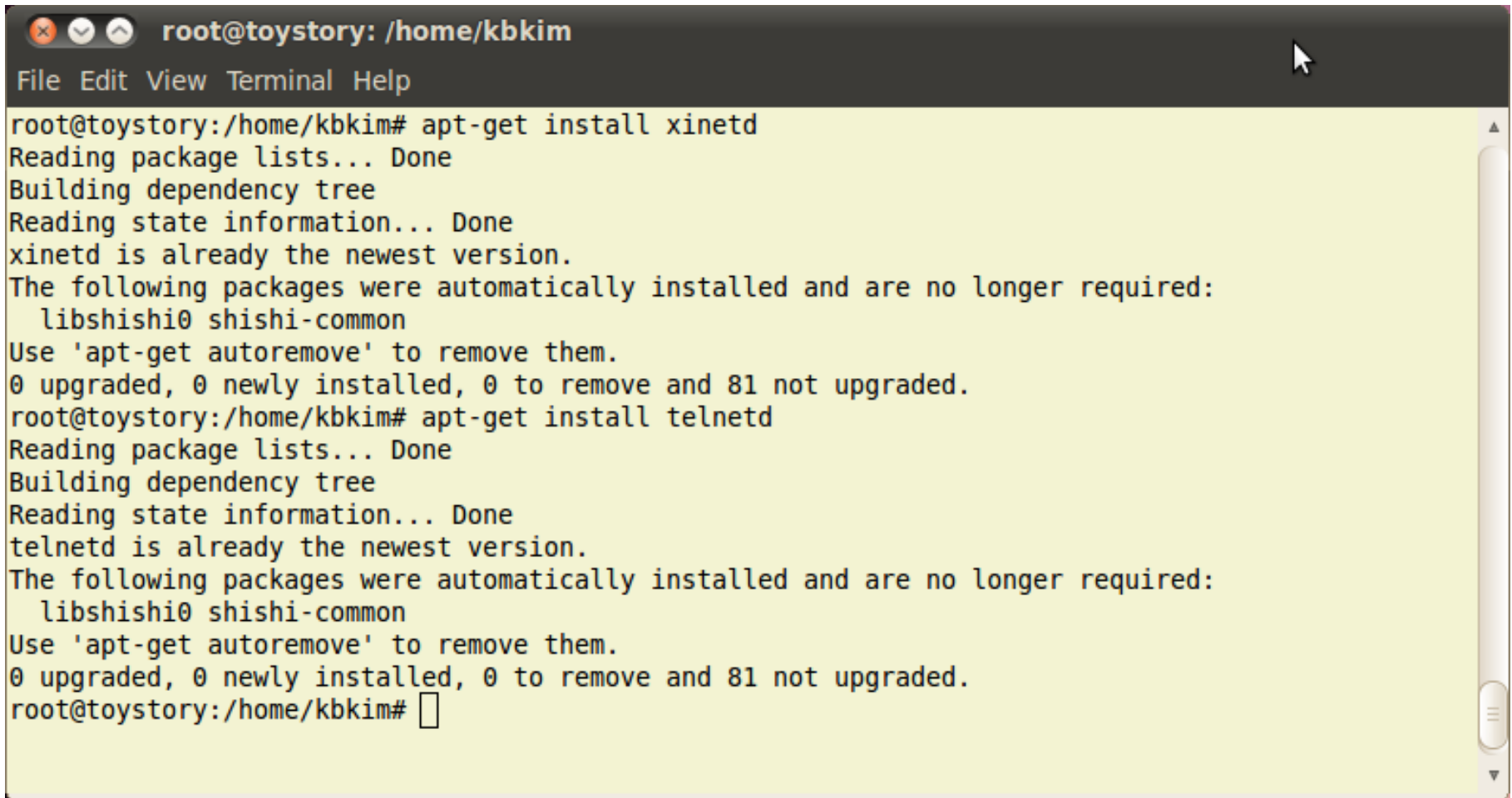
# Session

- Identify the connection between a client and a server
- A server assigns a **session ID** to a connection of a client
- Until the session ID is valid, a server identify a client which accessed the server before and re-access the server.
- Usually used in http with cookie.

# Telnet

- Text based remote access protocol
  - Use 23 port
- Client program
  - “telnet”
    - Usage : o [IP address]  
→ connect the machine with the given IP address
  - Basically provided in Linux distribution
- Server program
  - “telnetd”
  - Root needs to install “xinetd” and “telnetd”
  - Also needs to modify xinetd configuration

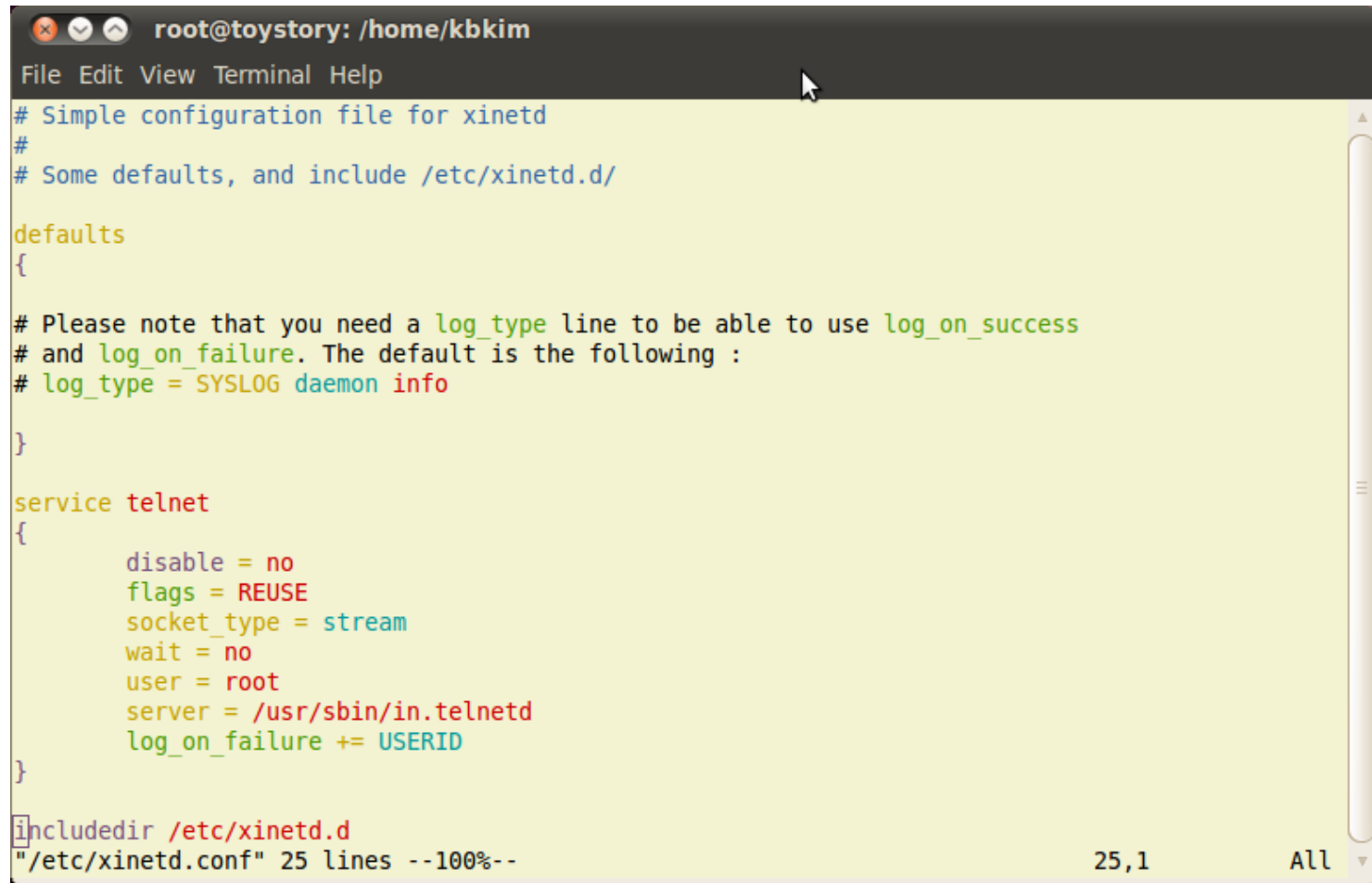
# Installing telnet server



A terminal window titled "root@toystory: /home/kbkim" with a menu bar (File, Edit, View, Terminal, Help). The terminal output shows two attempts to install packages using apt-get. The first attempt to install xinetd shows it is already installed. The second attempt to install telnetd also shows it is already installed. Both attempts list automatically installed packages (libshishi0, shishi-common) and suggest using 'apt-get autoremove' to remove them. The terminal ends with a prompt and a cursor.

```
root@toystory: /home/kbkim
File Edit View Terminal Help
root@toystory:/home/kbkim# apt-get install xinetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
xinetd is already the newest version.
The following packages were automatically installed and are no longer required:
  libshishi0 shishi-common
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 81 not upgraded.
root@toystory:/home/kbkim# apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnetd is already the newest version.
The following packages were automatically installed and are no longer required:
  libshishi0 shishi-common
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 81 not upgraded.
root@toystory:/home/kbkim#
```

# Modify xinetd configuration

A screenshot of a terminal window with a dark title bar. The title bar contains window control icons and the text 'root@toystory: /home/kbkim'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The main area of the terminal displays the contents of the xinetd configuration file, which is syntax-highlighted. The configuration includes comments, a 'defaults' block, a 'service telnet' block with various settings, and an 'includedir' statement. The status bar at the bottom shows the cursor position at line 25, column 1, and indicates that all 25 lines of the file are visible at 100% zoom.

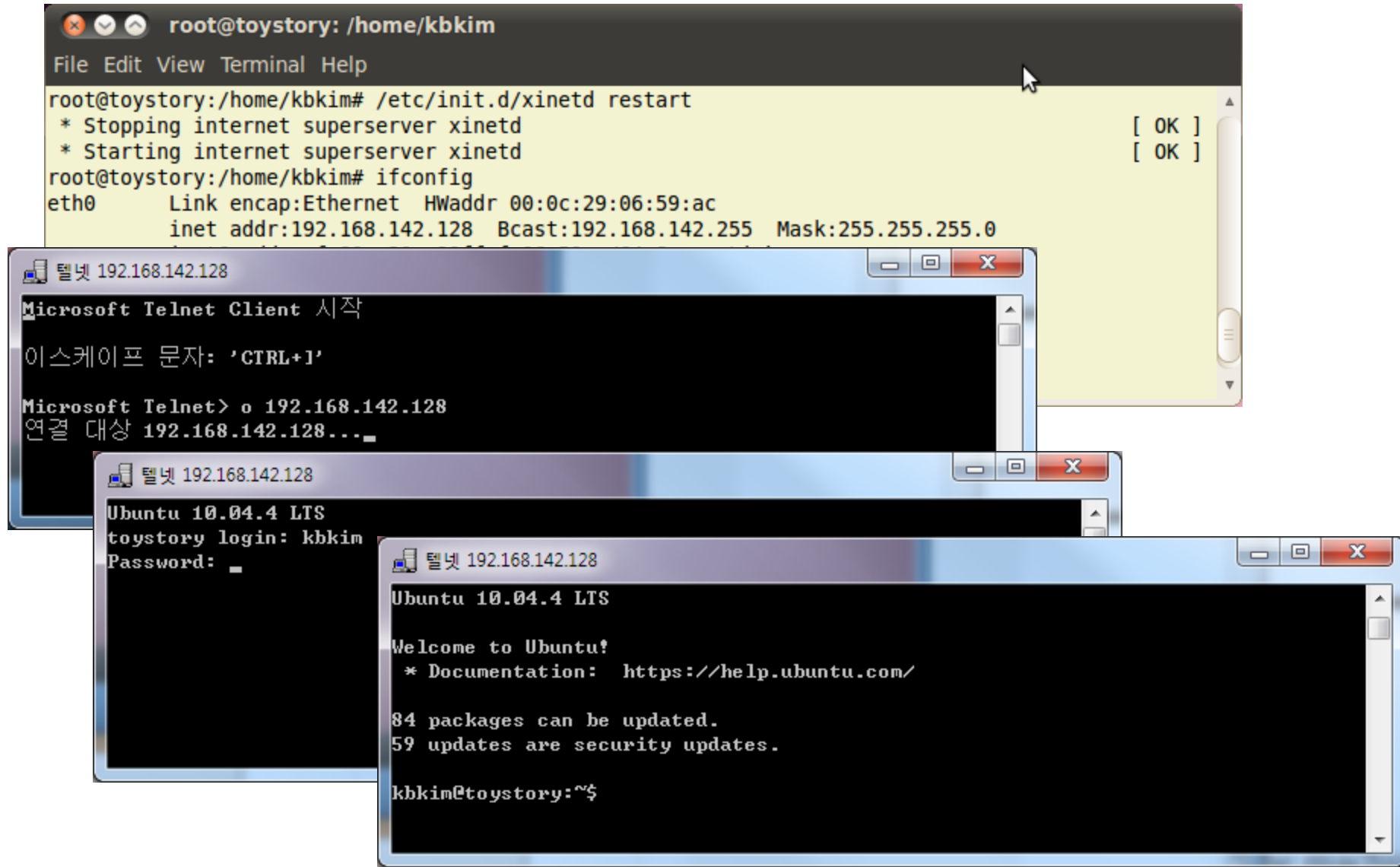
```
root@toystory: /home/kbkim
File Edit View Terminal Help
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    # Please note that you need a log_type line to be able to use log_on_success
    # and log_on_failure. The default is the following :
    # log_type = SYSLOG daemon info
}

service telnet
{
    disable = no
    flags = REUSE
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/in.telnetd
    log_on_failure += USERID
}

includedir /etc/xinetd.d
"/etc/xinetd.conf" 25 lines --100%-- 25,1 All
```

# Run telnet server and use telnet



The image shows three overlapping terminal windows. The top window is a Linux terminal with the prompt `root@toystory: /home/kbkim`. It shows the command `/etc/init.d/xinetd restart` being executed, which stops and then starts the xinetd service. It also shows the output of `ifconfig` for the `eth0` interface, showing an IP address of `192.168.142.128`. The middle window is a Microsoft Telnet Client titled "텔넷 192.168.142.128". It shows the command `o 192.168.142.128` being entered, and the connection status "연결 대상 192.168.142.128...". The bottom window is another Microsoft Telnet Client titled "텔넷 192.168.142.128". It shows the login process for "kbkim" on "Ubuntu 10.04.4 LTS", including the password prompt and the resulting shell prompt `kbkim@toystory:~$`.

```
root@toystory: /home/kbkim
File Edit View Terminal Help
root@toystory:/home/kbkim# /etc/init.d/xinetd restart
* Stopping internet superserver xinetd      [ OK ]
* Starting internet superserver xinetd      [ OK ]
root@toystory:/home/kbkim# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:06:59:ac
          inet addr:192.168.142.128  Bcast:192.168.142.255  Mask:255.255.255.0

Microsoft Telnet Client 시작
이스케이프 문자: 'CTRL+I'

Microsoft Telnet> o 192.168.142.128
연결 대상 192.168.142.128...

Ubuntu 10.04.4 LTS
toystory login: kbkim
Password: 
kbkim@toystory:~$
```

# Change of status of network

```
root@toystory: /home/kbkim
File Edit View Terminal Help

root@toystory:/home/kbkim# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 localhost.localdom:3350  *:*                    LISTEN
tcp      0      0 *:telnet                *:*                    LISTEN
tcp      0      0 localhost.localdoma:ipp  *:*                    LISTEN
tcp      0      0 *:3389                  *:*                    LISTEN
tcp      0      0 toystory.local:telnet    192.168.142.1:50171    ESTABLISHED
tcp6     0      0 localhost:ipp           [::]:*                 LISTEN

root@toystory:/home/kbkim# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 localhost.localdom:3350  *:*                    LISTEN
tcp      0      0 *:telnet                *:*                    LISTEN
tcp      0      0 localhost.localdoma:ipp  *:*                    LISTEN
tcp      0      0 *:3389                  *:*                    LISTEN
tcp      0      0 toystory.local:telnet    192.168.142.1:50171    TIME_WAIT
tcp6     0      0 localhost:ipp           [::]:*                 LISTEN

root@toystory:/home/kbkim# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 localhost.localdom:3350  *:*                    LISTEN
tcp      0      0 *:telnet                *:*                    LISTEN
tcp      0      0 localhost.localdoma:ipp  *:*                    LISTEN
tcp      0      0 *:3389                  *:*                    LISTEN
tcp6     0      0 localhost:ipp           [::]:*                 LISTEN

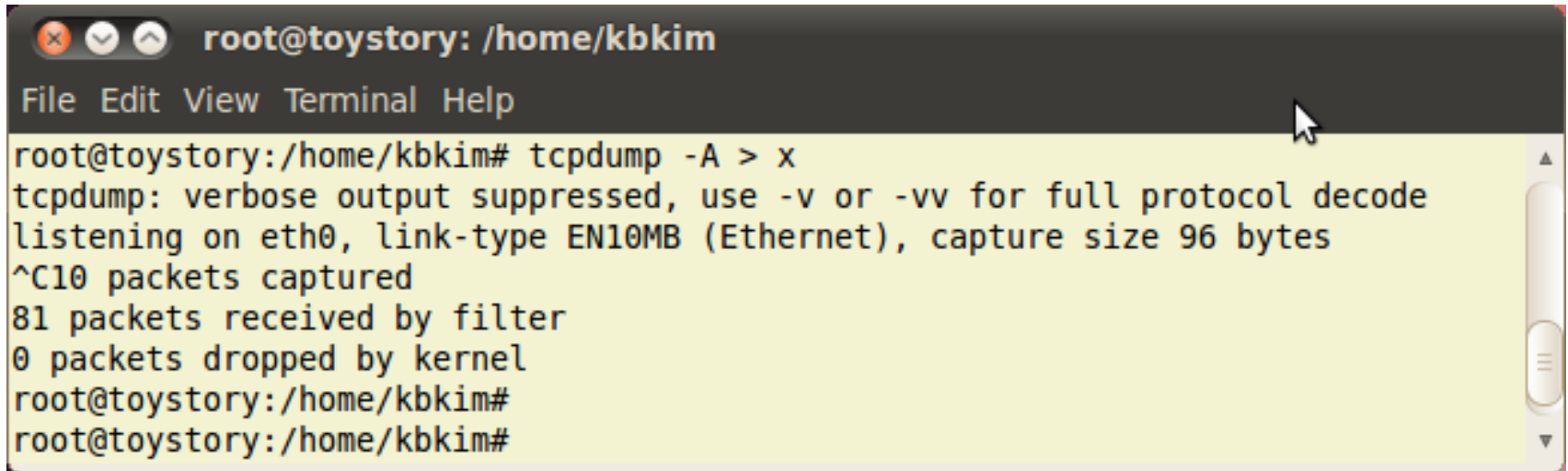
root@toystory:/home/kbkim# /etc/init.d/xinetd stop
* Stopping internet superserver xinetd
root@toystory:/home/kbkim#
```

During Telnet Connection Established

After Telnet Connection Closed



# Eavesdropping password over telnet

A terminal window titled 'root@toystory: /home/kbkim' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the execution of 'tcpdump -A > x', which starts listening on eth0. It then shows a Ctrl-C interrupt, followed by statistics: 10 packets captured, 81 received by filter, and 0 dropped by kernel. The prompt returns to root@toystory: /home/kbkim#.

```
root@toystory: /home/kbkim
File Edit View Terminal Help
root@toystory:/home/kbkim# tcpdump -A > x
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
^C10 packets captured
81 packets received by filter
0 packets dropped by kernel
root@toystory:/home/kbkim#
root@toystory:/home/kbkim#
```

# Your Login name and Password are revealed!!

root@toystory: /home/kbkim

File Edit View Terminal Help

07:48:38.377229 IP 192.168.142.2.domain > toystory.local.59067: E..&z...u.....5.....C.....e.8.0.3.4.2.1.a.b.9.1.c.  
07:48:38.836670 IP 192.168.142.1.50534 > toystory.local.telnet: 2, win 256, length 1  
E..)#@...X.....f..s.='&'..)P....N..k....  
07:48:38.836695 IP toystory.local.telnet > 192.168.142.1.50534: length 0  
E..(q.@.@+R.....f'..)s='P..\....  
07:48:38.841859 IP toystory.local.telnet > 192.168.142.1.50534: 0, win 92, length 1  
E..)q.@.+P.....f'..)s='P..\....k  
07:48:38.991049 IP 192.168.142.1.50534 > toystory.local.telnet: 3, win 256, length 1  
E..).\$@...X.....f..s=.''\*.P....L..b....  
07:48:38.997877 IP toystory.local.telnet > 192.168.142.1.50534: 1, win 92, length 1  
E..)q.@.+O.....f'..'s=(P..\....b  
07:48:39.103629 IP 192.168.142.1.50534 > toystory.local.telnet: 4, win 256, length 1  
E..).%@...X.....f..s=('..+P....J..k....  
07:48:39.109891 IP toystory.local.telnet > 192.168.142.1.50534: 2, win 92, length 1  
E..)q.@.+N.....f'..'s=.)P..\....k  
07:48:39.303917 IP 192.168.142.1.50534 > toystory.local.telnet: length 0  
E..(.&@...X.....f..s=.)'...',P....Q.....  
07:48:39.311553 IP 192.168.142.1.50534 > toystory.local.telnet: 5, win 256, length 1  
E..).'@...X.....f..s=.)'...',P....H..i....  
07:48:39.317915 IP toystory.local.telnet > 192.168.142.1.50534: 3, win 92, length 1  
E..)q.@.+M.....f'..'s=.\*P..\....i  
07:48:39.403369 IP 192.168.142.1.50534 > toystory.local.telnet: 6, win 256, length 1  
E..).(@...X.....f..s=.\*'...-P....F..m....  
07:48:39.409878 IP toystory.local.telnet > 192.168.142.1.50534: 4, win 92, length 1  
E..)q.@.+L.....f'...'s=+P..\....m  
07:48:39.545471 IP 192.168.142.1.50534 > toystory.local.telnet: 7, win 256, length 2

root@toystory: /home/kbkim

File Edit View Terminal Help

E..2q.@.@+A.....f'..'s=-.P..\....  
.Password:  
07:48:39.943930 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [..], ack 99, win 256, length 0  
E..(+@...X.....f..s=-.'..:P....?.....  
07:48:40.154966 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [P.], seq 66:67, ack 99, win 256, length 1  
E..)..@...X.....f..s=-.'..:P....6..1....  
07:48:40.193919 IP toystory.local.telnet > 192.168.142.1.50534: Flags [..], ack 67, win 92, length 0  
E..(q.@.+J.....f'..'s=..P..\....  
07:48:40.392669 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [P.], seq 67:68, ack 99, win 256, length 1  
E..).-@...X.....f..s=-.'..:P....5..2....  
07:48:40.392687 IP toystory.local.telnet > 192.168.142.1.50534: Flags [..], ack 68, win 92, length 0  
E..(q.@.+I.....f'..'s=/P..\....  
07:48:40.625178 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [P.], seq 68:69, ack 99, win 256, length 1  
E..)..@...X.....f..s=/.'..:P....4..3....  
07:48:40.625199 IP toystory.local.telnet > 192.168.142.1.50534: Flags [..], ack 69, win 92, length 0  
E..(q.@.+H.....f'..'s=.0P..\....  
07:48:40.850827 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [P.], seq 69:70, ack 99, win 256, length 1  
E..)./@...X.....f..s=.0'..:P....3..4....  
07:48:40.850867 IP toystory.local.telnet > 192.168.142.1.50534: Flags [..], ack 70, win 92, length 0  
E..(q.@.+G.....f'..'s=.1P..\....  
07:48:41.085065 IP 192.168.142.1.50534 > toystory.local.telnet: Flags [P.], seq 70:72, ack 99, win 256, length 2  
E..\*.0@...X.....f..s=.1'..:P....'..^M  
....  
07:48:41.085077 IP toystory.local.telnet > 192.168.142.1.50534: Flags [..], ack 72, win 92, length 0  
E..(q.@.+F.....f'..'s=.3P..\....  
07:48:41.093890 IP toystory.local.telnet > 192.168.142.1.50534: Flags [P.], seq 99:101, ack 72, win 92, length 2  
E..\*q.@.+C.....f'..'s=.3P..\....^M

241,10 84%

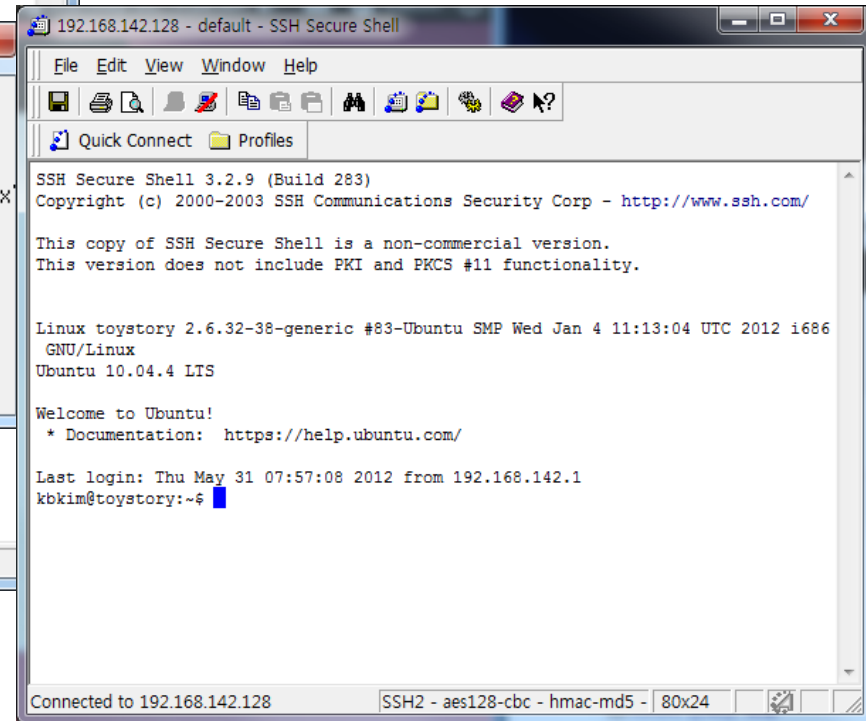
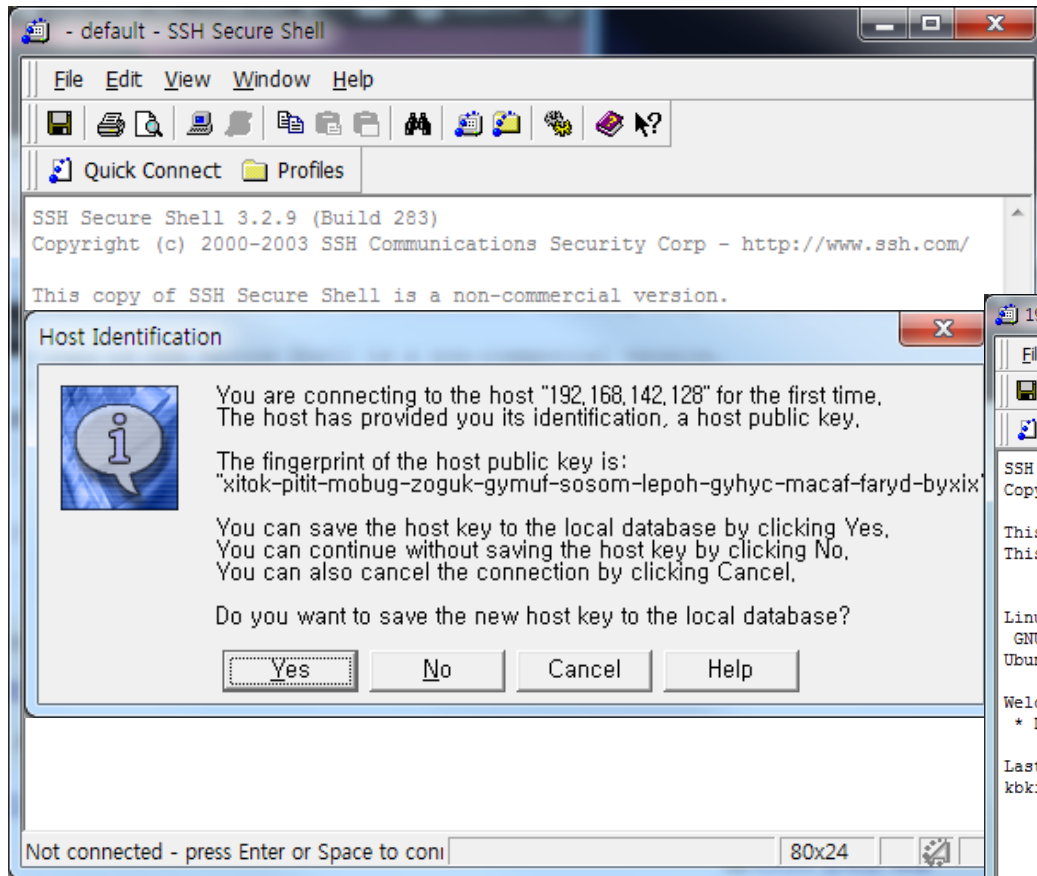
# SSH

- Telnet is relatively unsecure protocol
  - Use plain text for passing passwords
- SSH
  - Secure Shell → for secure data communication
    - Use 22 port
  - Establish a secure channel over an insecure network
  - Use public-key cryptography to authenticate the remote computer
    - Entire login session, including transmission of password is encrypted
  - It can be used for other applications
    - ftp → sftp, svn → ssh+svn, cp → scp

# Setup ssh server

```
root@toystory: /home/kbkim
File Edit View Terminal Help
root@toystory:/home/kbkim# apt-get install ssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
ssh is already the newest version.
The following packages were automatically installed and are no longer required:
  libshishi0 shishi-common
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 81 not upgraded.
root@toystory:/home/kbkim# service ssh restart
ssh start/running, process 4216
root@toystory:/home/kbkim# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3350          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3389            0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                     LISTEN
tcp6       0      0 :::1:631                 :::*                     LISTEN
root@toystory:/home/kbkim#
```

# ssh client



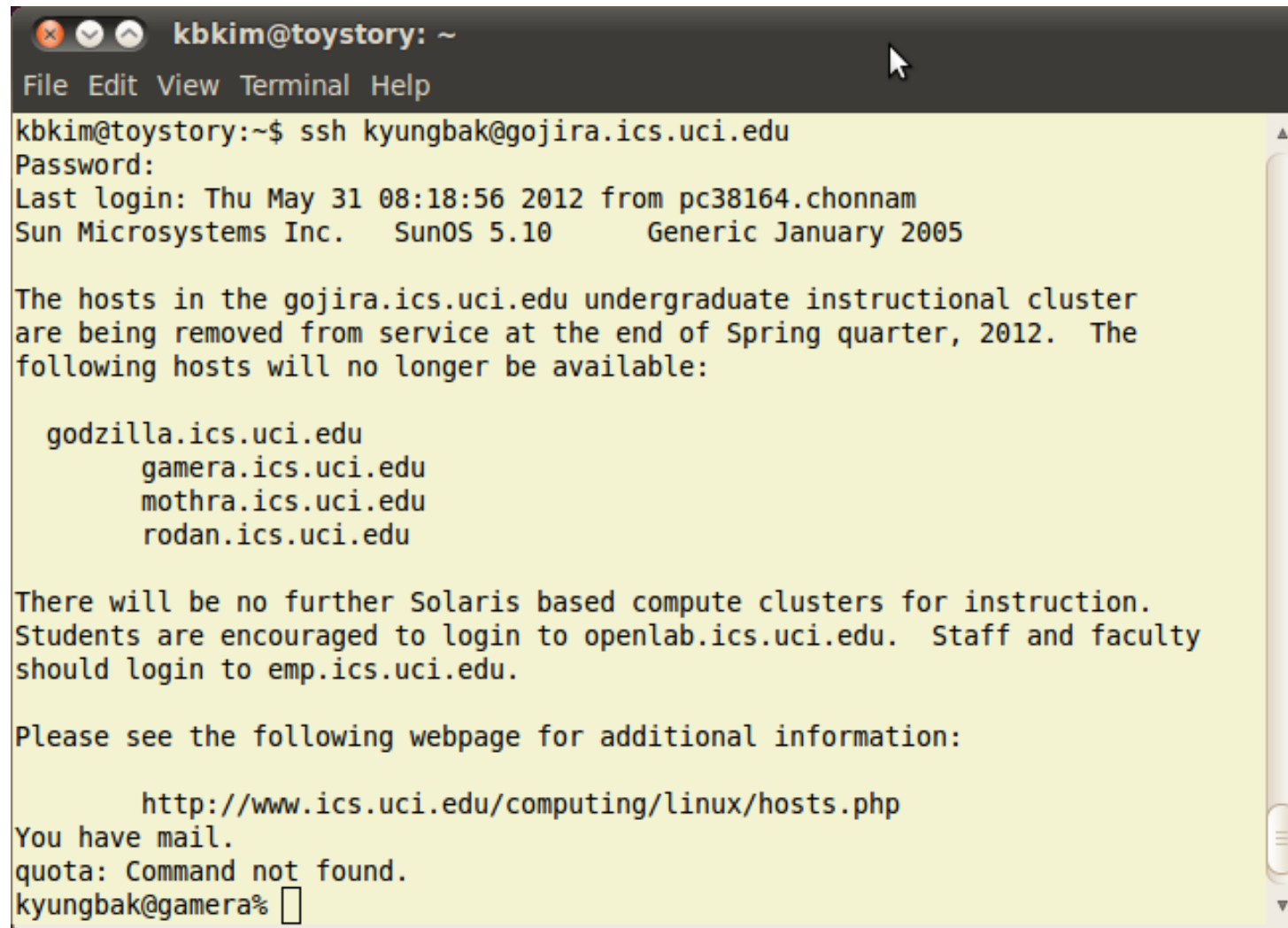
# Login information is encrypted

```
root@toystory: /home/kbkim
File Edit View Terminal Help
08:13:55.201212 IP toystory.local.ssh > 192.168.142.1.50901: Flags [P.], seq 1688:1736, ack 4013, win 227, length 48
E..Xd.@.@.7.....I.7g.Eu.P....;...n="s...bV..."...x.Ba...x:.....
08:13:55.201775 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [P.], seq 4013:4125, ack 1736, win 255, length 112
E....k@...W".....Eu.I.7.P...'...S.6g. ..VqV..v.....S..8(..[.=.6
08:13:55.201790 IP toystory.local.ssh > 192.168.142.1.50901: Flags [.], ack 4125, win 227, length 0
E..(d.@.@.8.....I.7..Eu.P...z[...
08:13:55.201841 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [P.], seq 4125:4205, ack 1736, win 255, length 80
E..x.l@...WA.....Eu.I.7.P....B...y...'..H...<d...j'~X.)..P.-:.....[
08:13:55.201858 IP toystory.local.ssh > 192.168.142.1.50901: Flags [.], ack 4205, win 227, length 0
E..(d.@.@.8.....I.7..EvDP...z...
08:13:55.202320 IP toystory.local.ssh > 192.168.142.1.50901: Flags [P.], seq 1736:1816, ack 4205, win 227, length 80
E..xd.@.@.7.....I.7..EvDP.....i\.">8.^M|.....).... t ...j.p.%(Jy.2
08:13:55.202718 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [P.], seq 4205:4301, ack 1816, win 255, length 96
E....m@...W0.....EvDI.7.P...n....8...y..k.....z...)..Dj...@.n....E.
08:13:55.202761 IP toystory.local.ssh > 192.168.142.1.50901: Flags [P.], seq 1816:2104, ack 4301, win 227, length 288
E..Hd.@.@.6.....I.7..Ev.P.....a..#p....nA.....79....[5.Rp.A..
08:13:55.333528 IP toystory.local.ssh > 192.168.142.1.50901: Flags [P.], seq 2104:2168, ack 4301, win 227, length 64
E..hd.@.@.7.....I.9..Ev.P.....$,...rm...u..T.L.!}....:7.!.Q.Y=....
08:13:55.333620 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [.], ack 2168, win 253, length 0
E..(.n@...W.....Ev.I.9GP...w.....
08:13:56.806011 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [P.], seq 4301:4381, ack 2168, win 253, length 80
E..x.o@...W>.....Ev.I.9GP...\\....R.q...Ts.....M...r.....20y....F..
08:13:56.813605 IP toystory.local.ssh > 192.168.142.1.50901: Flags [P.], seq 2168:2216, ack 4381, win 227, length 48
E..Xd.@.@.7.....I.9G.Ev.P...L..}5.C..8.xd.&...j.....H.....).1..
08:13:57.005592 IP 192.168.142.1.50901 > toystory.local.ssh: Flags [.] ack 2216, win 253, length 0
E..(.p@...W.....Ev.I.9wP...wa.....
08:13:57.142512 IP 192.168.142.1.50901 > toyst
E..x.q@...W<.....Ev.I.9wP...*a.....P..
08:13:57.149585 IP toystory.local.ssh > 192.16
E..Xd.@.@.7.....I.9w.EwDP...Q...
```

Your Password is safe over  
unsecure internet



# ssh client in Ubuntu



A screenshot of a terminal window in Ubuntu. The window title is 'kbkim@toystory: ~'. The menu bar shows 'File Edit View Terminal Help'. The terminal content shows an SSH session from 'kbkim@toystory' to 'kyungbak@gojira.ics.uci.edu'. It displays the password prompt, login history, system information (SunOS 5.10), and a notice about the removal of hosts from the gojira.ics.uci.edu cluster. A list of affected hosts is provided: godzilla.ics.uci.edu, gamera.ics.uci.edu, mothra.ics.uci.edu, and rodan.ics.uci.edu. It also mentions that Solaris-based clusters will no longer be used for instruction and provides a URL for more information. The session ends with 'You have mail.' and a 'quota: Command not found.' message. The prompt is now 'kyungbak@gamera%'.

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ ssh kyungbak@gojira.ics.uci.edu  
Password:  
Last login: Thu May 31 08:18:56 2012 from pc38164.chonnam  
Sun Microsystems Inc. SunOS 5.10 Generic January 2005  
  
The hosts in the gojira.ics.uci.edu undergraduate instructional cluster  
are being removed from service at the end of Spring quarter, 2012. The  
following hosts will no longer be available:  
  
    godzilla.ics.uci.edu  
        gamera.ics.uci.edu  
        mothra.ics.uci.edu  
        rodan.ics.uci.edu  
  
There will be no further Solaris based compute clusters for instruction.  
Students are encouraged to login to openlab.ics.uci.edu. Staff and faculty  
should login to emp.ics.uci.edu.  
  
Please see the following webpage for additional information:  
  
    http://www.ics.uci.edu/computing/linux/hosts.php  
You have mail.  
quota: Command not found.  
kyungbak@gamera% 
```

# Using public key

```
kbkim@toystory: ~/.ssh
File Edit View Terminal Help

kbkim@toystory:~/.ssh$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kbkim/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kbkim/.ssh/id_rsa.
Your public key has been saved in /home/kbkim/.ssh/id_rsa.pub.
The key fingerprint is:
27:e8:45:c6:b9:1b:9c:9b:e2:14:bf:90:7b:d8:3e:29 kbkim@toystory
The key's randomart image is:
+--[ RSA 2048 ]-----+
|
|   . .
|   =
|  = 0
| o S .
| . = B
| *0=.
| oE+=.
| o+0.
|
+-----+

kbkim@toystory:~/.ssh$ ls
id_rsa id_rsa.pub known_hosts
kbkim@toystory:~/.ssh$ touch authorized_keys
kbkim@toystory:~/.ssh$ ls
authorized_keys id_rsa id_rsa.pub known_hosts
kbkim@toystory:~/.ssh$
```

For users who do not need to provide passwords



# Contents of known\_hosts and rsa key

```
kbkim@toystory: ~/.ssh
File Edit View Terminal Help

kbkim@toystory:~/.ssh$ cat known_hosts
|1|28rAEVsc2sozKnt5pjf+JaTFdHo=|k+BmYNGERaynkuUemXnpqMJv0Qs= ssh-rsa AAAAB3NzaC
1yc2EAAAABIwAAAIEA4F/SBcCRg/DLM4ytKUPKcaDgi0E35dWG4EbuTetqVhpdqBjgcFy/q3eulinIv
6alNeYQKEWb2CbuUyHA6l7+JOWp06va017C8CDKw+TNaxtEtzZ7wtqQglg2G/Gvvw7/V5Xq9jL9lqwu
ls/CSYdwb4tl0x5SC2ujq0WvoZdpX8E=
|1|fFEEZCpmQkTDNjEdeCHs/9u8JA=|kTvzQp0GEFXx73bg3tSkCG7927A= ssh-rsa AAAAB3NzaC
1yc2EAAAABIwAAAIEA4F/SBcCRg/DLM4ytKUPKcaDgi0E35dWG4EbuTetqVhpdqBjgcFy/q3eulinIv
6alNeYQKEWb2CbuUyHA6l7+JOWp06va017C8CDKw+TNaxtEtzZ7wtqQglg2G/Gvvw7/V5Xq9jL9lqwu
ls/CSYdwb4tl0x5SC2ujq0WvoZdpX8E=
|1|Uhj3jtNvrg344uooruY2BGQOm04=|+rTXeX0KtlgB4x3Lwz07mSkGjKk= ssh-rsa AAAAB3NzaC
1yc2EAAAABIwAAAIEA4F/SBcCRg/DLM4ytKUPKcaDgi0E35dWG4EbuTetqVhpdqBjgcFy/q3eulinIv
6alNeYQKEWb2CbuUyHA6l7+JOWp06va017C8CDKw+TNaxtEtzZ7wtqQglg2G/Gvvw7/V5Xq9jL9lqwu
ls/CSYdwb4tl0x5SC2ujq0WvoZdpX8E=

kbkim@toystory:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAqsjIeYNf3iwKv+HYy34C193aUHKFnzYTMHKosq5wHAg
8bqGVYIbRYvDpoeAsfVSxthswUMJyl8ZqnVVI24WJ5iaDwFUI4a+6cSy8FjR5LrWw7nBYzaa4sQLTgV
3rkjreqvdgmdl3lV27UFxd3oTxGKekGxuF3grf1ArpmE3h5QadwK7a0aFsFdNwzUTn20xvNK7unlkH3
ubW8kQSKV+UT+QDuxkEcJG50w/DHLJQBF7yalseen0pgjFWP1WnJ6nxKo/PVUHq/DY0/2r/rqrm7Nc0
kzGTyagi8K7laGJIgmtuVL8yEx3kn3M5Smj+PI+4veJlfi/MyyDlsd2IdnBq/w== kbkim@toystory
kbkim@toystory:~/.ssh$
```

Key for  
Machines

Key for  
Users

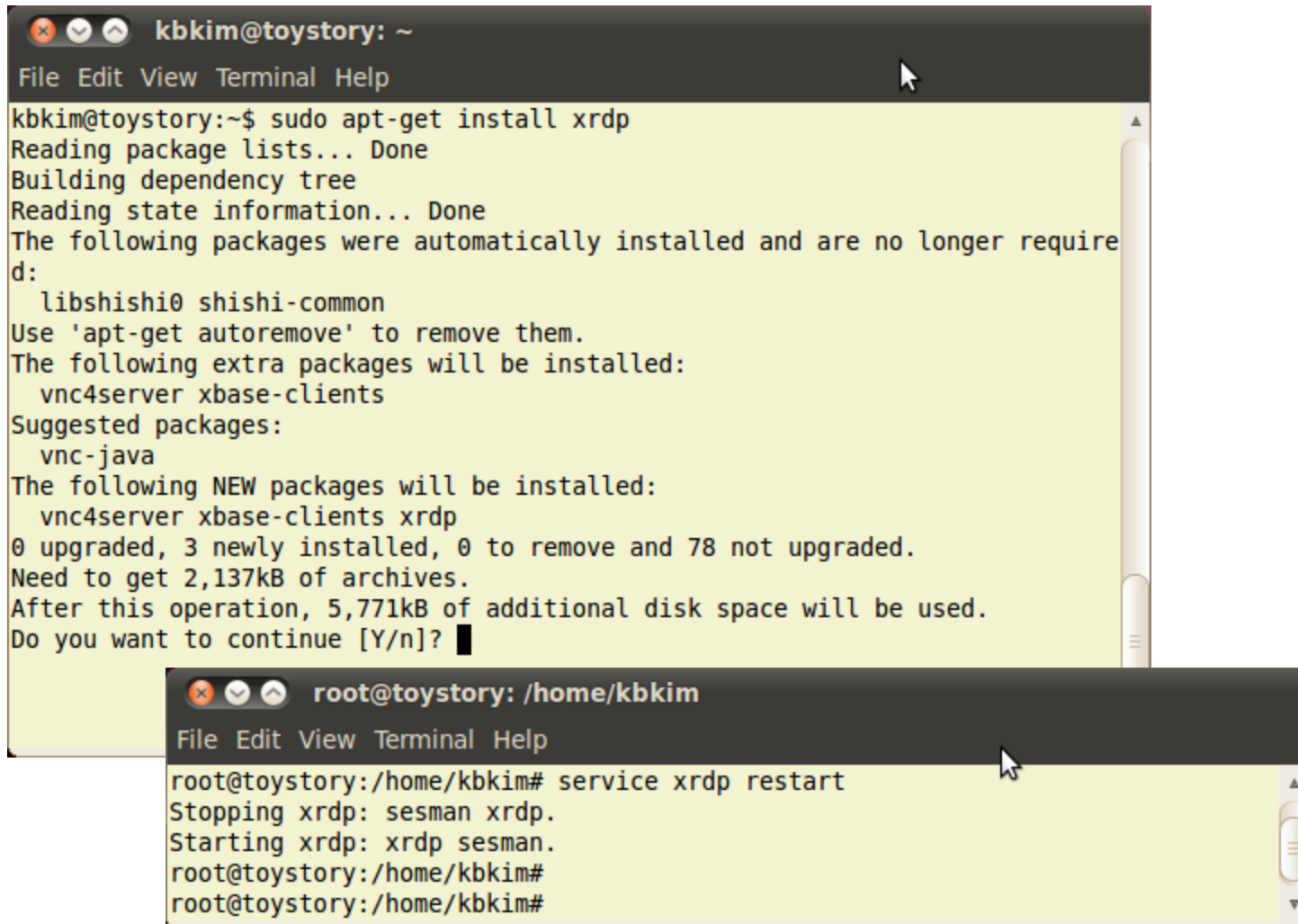
kbkim@toystory\$ cat id\_rsa.pub >> authorized\_keys  
➔ After this command user “kbkim” does not need to provide password to establish ssh connection.

# Remote Desktop



- A client accesses a server machine with a desktop environment
- RDP : Remote Desktop Protocol
  - Developed by Microsoft
  - Client exist for most version of MS windows, Linux, Unix, Mac OS X, Androd
  - TCP port : 3389
- Server deamon in Ubuntu
  - xrdp with sesman (session manager)

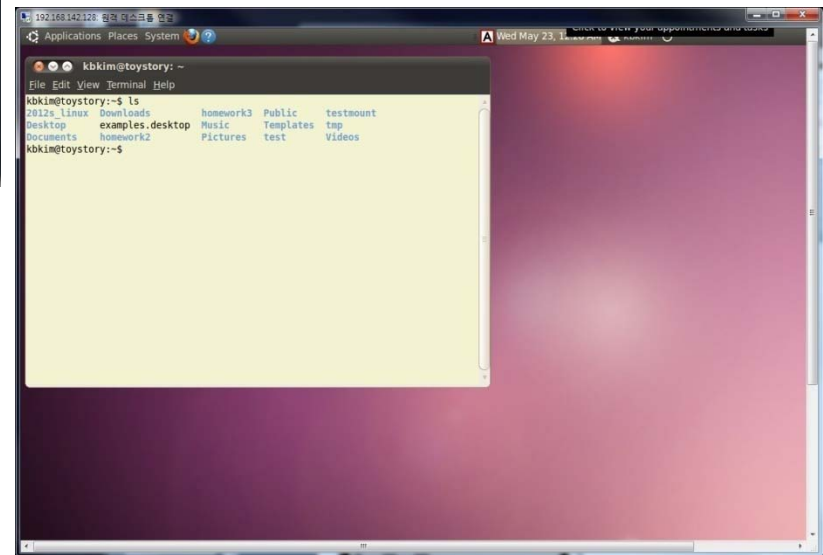
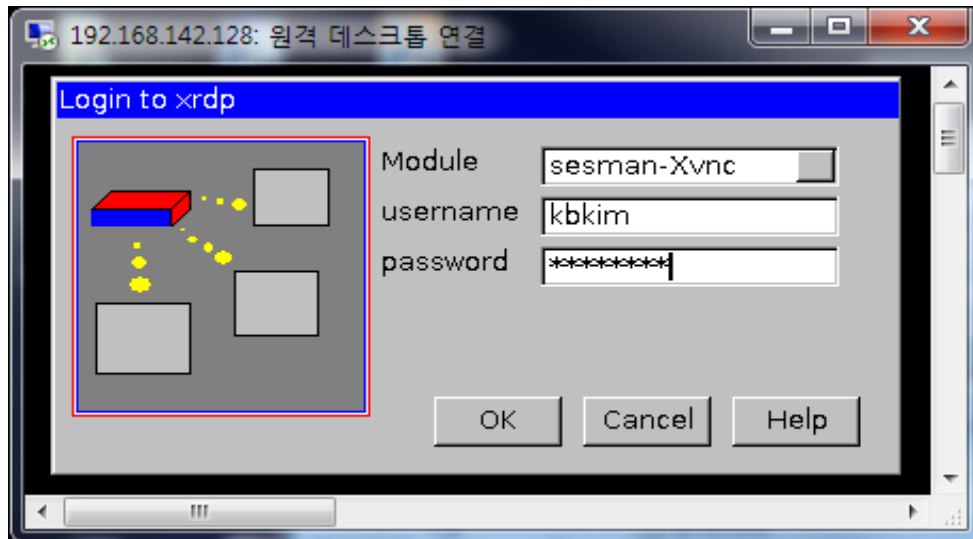
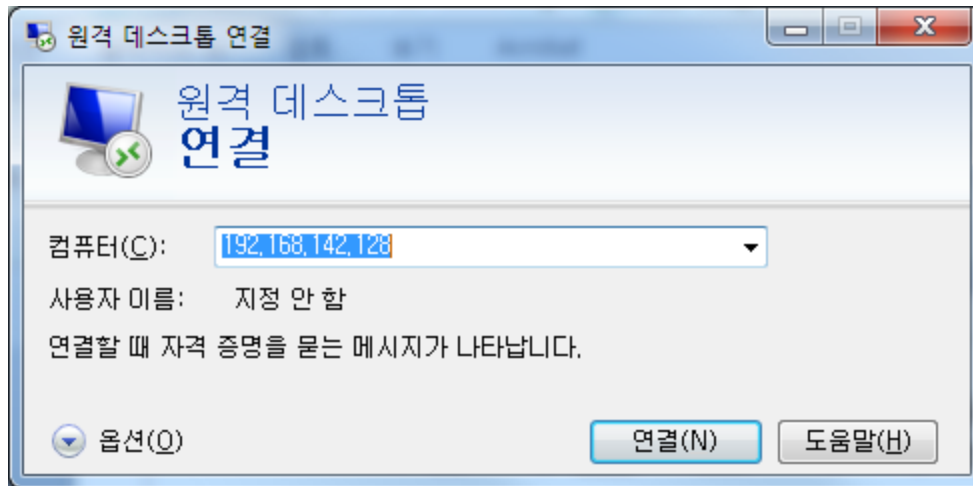
# Example of installation of xrdp



The image shows two terminal windows. The top window, titled 'kbkim@toystory: ~', shows the command 'sudo apt-get install xrdp' being executed. The output indicates that several extra packages (vnc4server, xbase-clients) will be installed along with xrdp. The bottom window, titled 'root@toystory: /home/kbkim', shows the command 'service xrdp restart' being executed, which successfully stops and starts the xrdp service.

```
kbkim@toystory: ~  
File Edit View Terminal Help  
kbkim@toystory:~$ sudo apt-get install xrdp  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libshishi0 shishi-common  
Use 'apt-get autoremove' to remove them.  
The following extra packages will be installed:  
  vnc4server xbase-clients  
Suggested packages:  
  vnc-java  
The following NEW packages will be installed:  
  vnc4server xbase-clients xrdp  
0 upgraded, 3 newly installed, 0 to remove and 78 not upgraded.  
Need to get 2,137kB of archives.  
After this operation, 5,771kB of additional disk space will be used.  
Do you want to continue [Y/n]?   
  
root@toystory: /home/kbkim  
File Edit View Terminal Help  
root@toystory:/home/kbkim# service xrdp restart  
Stopping xrdp: sesman xrdp.  
Starting xrdp: xrdp sesman.  
root@toystory:/home/kbkim#  
root@toystory:/home/kbkim#
```

# Client Side



# ftp server

- File transfer protocol
- VsFTP server
  - Installation : `# apt-get install vsftpd`
  - How to run : `# service vsftpd start/stop/restart`
  - Configuration of vsftp
    - Configuration File : `/etc/vsftpd.conf`
    - User login : allow users for connecting to ftp server
      - `Local_enable = YES`
    - Chroot : restrict user directory
      - `Chroot_local_user = YES`
    - Upload/write option
      - `Write_enable=YES`

# ftp server : anonymous users


- Anonymous user setting
  - Allow anonymous users
    - Anonymous\_enable=YES
  - Set the directory of anonymous users
    - Anon\_root=/var/ftp
  - Use password for anonymous users
    - Secure\_email\_list\_enable=YES
  - Allow update or write from anonymous users
    - Anon\_upload\_enable=YES
  - Allow delete or rename from anonymous users
    - Anon\_other\_write\_enable=YES

# Samba server

- A free software re-implementation of the SMB/CIFS networking protocol
- Provides file and printer services for various Microsoft Windows clients
- Samba runs on most Unix and Unix-like systems, such as Linux, Solaris, and BSD variants

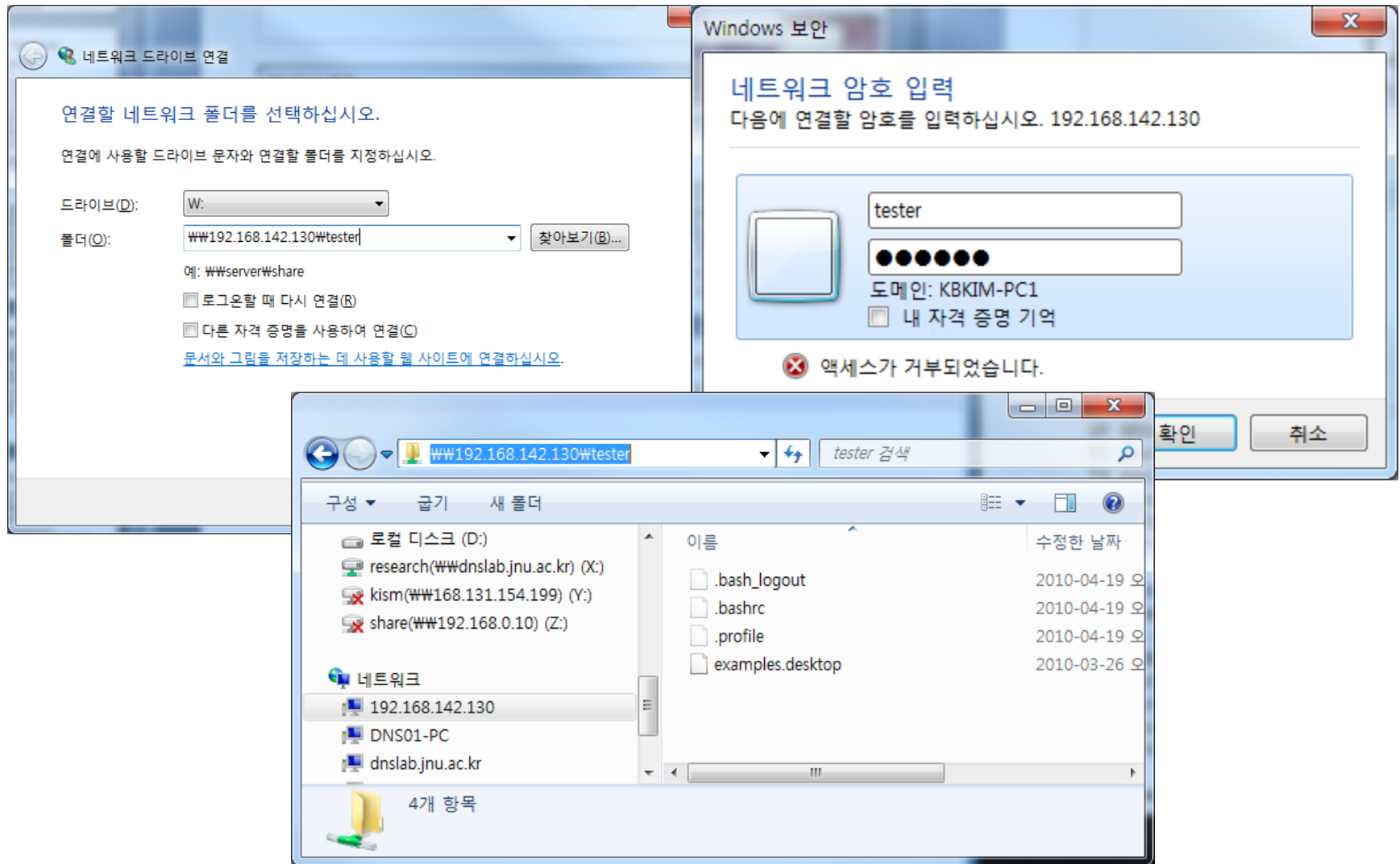
# Using Samba Server

- Installation : `# apt-get install samba smbfs`
  - How to run : `# service smbd restart/start/stop`
  - Configuration of samba server
    - Configuration file : `/etc/samba/smb.conf`
    - Authentication setting
      - `Security=user`
      - `Username map=/etc/samba/smbusers`
        - Need to set samba password for a user and indicate the user on `/etc/samba/smbusers` file
        - e.g., `# smbpasswd -a kbkim`
    - Sharing setting
      - `[homes]`
      - `comment = Home Directories`
      - `browseable = no`
      - `valid users = %S`
      - `read only = yes` or `Writable = yes`
- [any directory]**  
**path = /var/any/directory**  
**valid users = anyuser otheruser**  
**browseable = no**  
**writable = yes**  
**public = yes**  
**create mask = 0660**  
**directory mask = 0770**





# Example of Samba

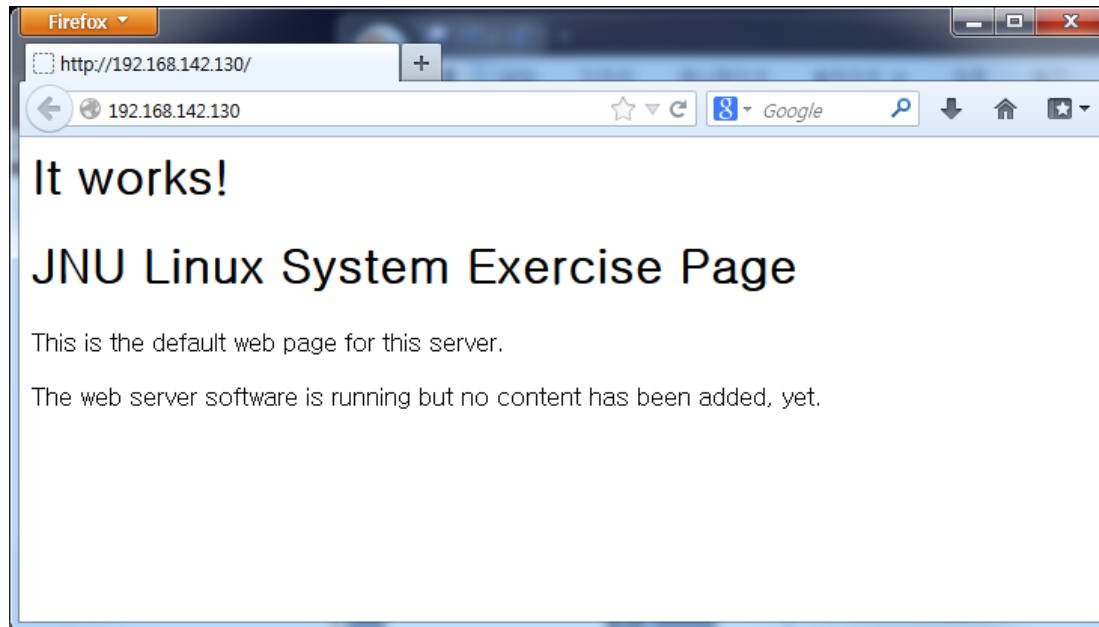


# Apache2 http server

- Web server software program, notable for playing a key role in the initial growth of the WWW.
- Typically Apache runs on a Unix-like operating system, and was developed for use on Linux
- Developed and maintained by an open community of developers under the auspices of the Apache Software Foundation

# Using Apache Web Server


- Installation : `# apt-get install apache2`
- How to run : `# service apache2 restart/start/stop`
- The home location of your web server
  - Default : `/var/www`
  - You can see the `index.html` in here



# Configuration of Apache Web Server

- Configuration
  - Configuration folder : `/etc/apache2`
    - Sub directories and files are for configuration of Apache Web Server
    - `apache2.conf` : main configuration
    - `mods-available` : available server modules
    - `mods-enabled` : enabled server modules
      - Symbolic links to point available modules
    - `sites-available/sites-enabled` : site configuration

# Allowing users' web page

- Enable user directory modules 
  - # ln -s /etc/apache2/mods-available/userdir.load /etc/apache2/mods-enabled/userdir.load
  - # ln -s /etc/apache2/mods-available/userdir.conf /etc/apache2/mods-enabled/userdir.conf
  - # service apache2 restart
- Prepare web contents at user side
  - Create “public\_html” directory under home directory of a user
  - Create “index.html” under “public\_html” directory
  - NOTE!! The file permission should be 755 for web directories 644 for web files

