DEPARTMENT OF INFORMATION TECHNOLOGY

COMPUTER COMMUNICATION AND NETWORKING LAB

LAB1: 25/7/2019

Objective

• Identify tools used to discover a computer network configuration with various operating

systems.

• Gather information including connection, host name, Layer 2 MAC address and Layer 3

TCP/IP network address information.

• Compare network information to other PCs on the network.

PC NETWORK AND TCP/IP CONFIGURATION

Open Terminal/command prompt

Step 1: Gather TCP/IP configuration information

In command prompt type **ifconfig** and press enter key.
The following figure shows the Command screen. Type ifconfig and press the Enter key.

```
himanshu@ansh:~$ ifconfig
enp3s0    Link encap:Ethernet  HWaddr 70:4d:7b:70:d2:3e
          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)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:73925 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73925 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7911049 (7.9 MB)  TX bytes:7911049 (7.9 MB)

wlx18a6f713679b Link encap:Ethernet  HWaddr 18:a6:f7:13:67:9b
          inet addr:192.168.2.6  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::733f:7699:a8de:78ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:598724 errors:0 dropped:5949 overruns:0 frame:0
          TX packets:481412 errors:0 dropped:20 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390451501 (390.4 MB)  TX bytes:102506204 (102.5 MB)
```

This screen shows the IP address (inet addr and inet6 addr), subnet mask (Mask), Hardware address(HWaddr).

Step 2: Identify the Default gateway

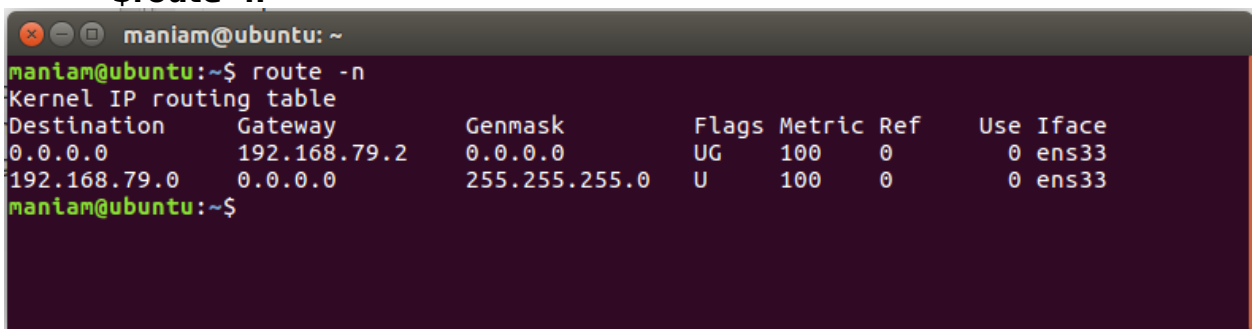
$ip r |grep default

The IP address and the default gateway should be in the same network or subnet, otherwise this host would not be able to communicate outside the network. In the figure the subnet mask tells us that the first three octets must be the same to be in the same network.

Note: If this computer is on a LAN, the default gateway might not be seen if it is running behind a Proxy Server.

Step 3: Finding routing table

$route -n



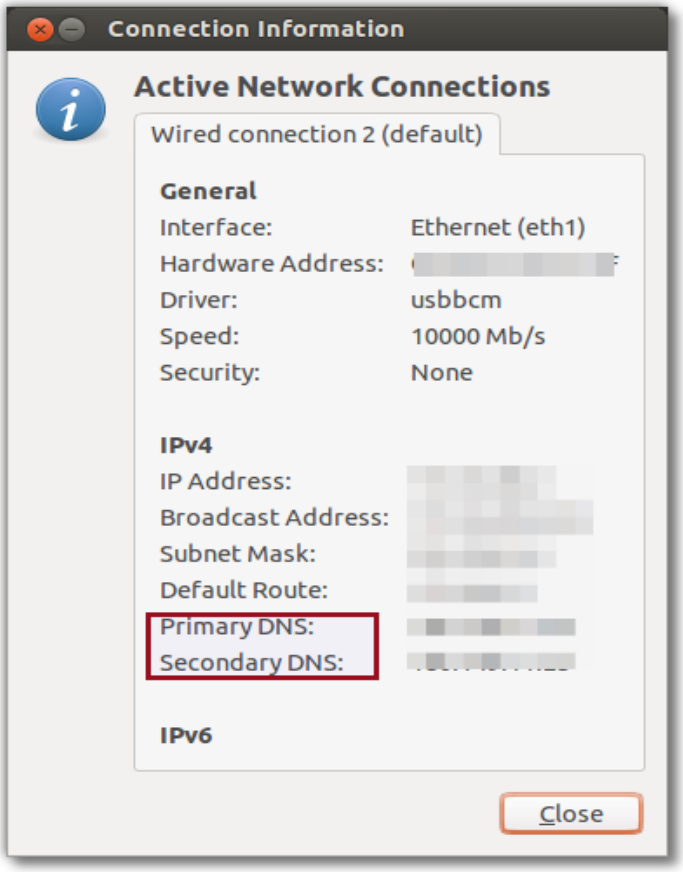
Step 4: Finding server details

```
$ nmcli dev show | grep 'DNS'
```

OR

1. Click on the Network connectivity icon on the top panel.
2. Select *Connection information*

The information will be as shown below



Step 4: Record the following TCP/IP information for your computer
IPv4 address : .....
IPv6 address: .....
Subnet Mask: .....
Default Gateway: .....
Hardware address: .....
Primary DNS:.....
Secondary DNS: .....
DHCP Server:.....

Step 5: Compare the TCP/IP configuration of this computer to others on the LAN
If this computer is on a LAN, compare the information of several machines.

Are there any similarities? _____
What is similar about the IP addresses? _____
What is similar about the default gateways? _____
The IP addresses should share the same network portion. All machines in the LAN should share the same default gateway.
Record a couple of the IP Addresses:.....

Also, the DHCP server address, if used, and the date the IP lease starts and ends should be displayed. Look over the information. Entries for the DNS, used in name resolution servers, may also be present.

Notice the Physical Address (MAC) and the NIC model (Description).

In the LAN, what similarities about the Physical (MAC) Addresses are seen?

While not a requirement, most LAN administrators try to standardize components like NICs. Therefore, it would not be surprising to find all machines share the first three Hex pairs in the adapter address. These three pairs identify the manufacturer of the adapter.

Write down the IP addresses of any servers listed: _____

Write down the computer Host Name: ($**hostname**)_____

Write down the Host Names of a couple other computers: _____

Do all of the servers and workstations share the same network portion of the IP address as the your workstation? _____

It would not be unusual for some or all of the servers and workstations to be in another network. It means that the computer default gateway is going to forward requests to the other network.

Reflection

Based on observations, what can be deduced about the following results taken from

three computers connected to one switch?

Computer 1

IP Address: 192.168.12.113

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Computer 2

IP Address: 192.168.12.205

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Computer 3

IP Address: 192.168.112.97

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Should they be able to talk to each other? _____

Are they all on the same network?_____

Why or why not? _____

USING PING AND TRACERT FROM A WORKSTATION

Objective

• Learn to use the TCP/IP Packet Internet Groper (ping) command from a workstation.

• Learn to use the Trace Route (tracert) command from a workstation.

• Observe name resolution occurrences using WINS and/or DNS servers.

step 1: Access the command prompt/Terminal

step 2: ping the IP address of another computer /domain name

example

ping 10.53.25.16

ping www.yahoo.com

The following figure shows the successful results of ping command.

```
bob@suse1:~> ping 192.168.198.130
PING 192.168.198.130 (192.168.198.130) 56(84) bytes of data.
64 bytes from 192.168.198.130: icmp_seq=1 ttl=64 time=6.14 ms
64 bytes from 192.168.198.130: icmp_seq=2 ttl=64 time=0.778 ms
64 bytes from 192.168.198.130: icmp_seq=3 ttl=64 time=0.599 ms
64 bytes from 192.168.198.130: icmp_seq=4 ttl=64 time=0.558 ms
64 bytes from 192.168.198.130: icmp_seq=5 ttl=64 time=0.615 ms
64 bytes from 192.168.198.130: icmp_seq=6 ttl=64 time=0.608 ms
64 bytes from 192.168.198.130: icmp_seq=7 ttl=64 time=0.645 ms
64 bytes from 192.168.198.130: icmp_seq=8 ttl=64 time=0.619 ms
64 bytes from 192.168.198.130: icmp_seq=9 ttl=64 time=0.698 ms
^C
--- 192.168.198.130 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8000ms
rtt min/avg/max/mdev = 0.558/1.252/6.149/1.732 ms
```

ping uses the ICMP echo reply feature to test physical connectivity. Since ping reports on four attempts, it gives an indication of the reliability of the connection. Look over the results and verify that the ping was successful. Is the ping successful? If not, perform check for different IP address.

Try to ping the IP address of the neighbour machine.

Note the results. _____

step 3: ping the IP address of the default gateway

Try to ping the IP address of the default gateway if one was listed in the last exercise. If the ping is successful, it means there is physical connectivity to the gateway on the local network and probably the rest of the world.

step 4: ping the IP address of a DHCP or DNS servers

Try to ping the IP address of any DHCP and/or DNS servers listed in the last exercise. If this works for either server, and they are not in the network, what does this indicate?

_____

Was the ping successful? _____

If not, perform appropriate troubleshooting.

step 5: ping the Loopback IP address of this computer

Type the following command: ping 127.0.0.1

The 127.0.0.0 network is reserved for loopback testing. If the ping is successful, then

TCP/IP is properly installed and functioning on this computer.

Was the ping successful? _____

If not, perform appropriate troubleshooting.

step 6: ping the hostname of another computer

Try to ping the hostname of the computer. Look over the results. Notice that the first line of output shows the host name, in the example, followed by the IP address. This means the computer was able to resolve the host name to an IP address. Without name resolution, the ping would have failed because TCP/IP only understands valid IP addresses, not names.

If the ping was successful, it means that connectivity and discovery of IP addresses can be done with only a hostname. In fact, this is how many early networks communicated.

step 7: ping the nitk website

ping nitk.ac.in

The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address.

A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses. Without this name resolution, the ping would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.

With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.

step 8: ping the Microsoft web site and Cisco website

Type the following command:

a. ping www.microsoft.com

b. ping www.cisco.com

Notice that the DNS server was able to resolve the name to an IP address, but there is no response. Some Microsoft and Cisco routers are configured to ignore ping requests. This is a frequently implemented security measure. Ping some other domain names and record the results.

step 9: Type traceroute www.cisco.com and press Enter.

traceroute is TCP/IP command for finding route. The preceding figure shows the successful result when running tracert to google.com.

```
prabhakar@Inspiron-3542:~$ traceroute google.com
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets
 1  192.168.43.45 (192.168.43.45)  2.014 ms  2.313 ms  2.588 ms
 2  * * *
 3  10.45.1.230 (10.45.1.230)  75.449 ms  115.244 ms  115.224 ms
 4  10.45.8.178 (10.45.8.178)  93.856 ms  115.138 ms  93.822 ms
 5  10.45.8.187 (10.45.8.187)  115.116 ms  115.106 ms  115.070 ms
 6  * * *
 7  218.248.235.141 (218.248.235.141)  120.589 ms  108.033 ms  106.962 ms
 8  218.248.235.142 (218.248.235.142)  114.489 ms * *
 9  72.14.211.114 (72.14.211.114)  98.076 ms  93.232 ms  93.781 ms
10  108.170.253.113 (108.170.253.113)  98.688 ms  91.388 ms 108.170.253.97 (108.170.253.97)  107.241 ms
11  74.125.253.69 (74.125.253.69)  95.120 ms 72.14.237.165 (72.14.237.165)  102.594 ms  103.137 ms
12  maa03s23-in-f14.1e100.net (172.217.26.206)  101.794 ms  97.987 ms  97.165 ms
prabhakar@Inspiron-3542:~$
```

The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the traceroute requests had to pass through to get to the destination. traceroute uses the same echo requests and replies as the ping command but in a

slightly different way. Observe that traceroute actually contacted each router three times. This is shown with the three different round trip time at each row.

Compare the results to determine the consistency of the route. Notice in the above example that there were relatively long delays after router 1 and 5, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity.

Each router represents a point where one network connects to another network and the packet was forwarded through.

step 10: trace route other IP addresses or domain addresses and record the results

step 11: Trace a local host name or IP address

Reflection

If the above steps are successful and ping or traceroute can verify connectivity with an Internet

Web site, what does this indicate about the computer configuration and about routers between the computer and the web site? _____

What is the job of default gateway? _____