**Technical Operations (TechOps)**

OS Admin

Linux Narrative Exercises

© FDM Group Ltd 2011. All Rights Reserved.

Any unauthorised reproduction or distribution in part  
or in whole will constitute an infringement of copyright.

|  |
| --- |
| Page left intentionally blank |

# Network Questions

Your instructor may choose to demonstrate these exercises because an error could leave your VM unusable.

First we run some commands to analyse the **layer 4** networking configuration.

Search the /etc/services file to find out which port is used to provide the ssh service. By the way, the putty software you are using to connect to Linux from Windows uses ssh.

grep ssh /etc/services

This shows the ssh is configured to listen on port 22 using the TCP protocol.

Now we want to see if we do in fact have a process listen on this port. We already know that we must have because we are connected using putty! Run the command

netstat –altn | grep ':22'

Note –a = all

-l = listening

-t = tcp

How many lines do you see?

3 (could vary)

Note words 'LISTEN' & 'ESTABLISHED' in the right most column?

To what does the output of the line saying 'ESTABLISHED' refer? What do you think it is talking about?

My current ssh connection I am using right now!

What are the two 'LISTEN' entries about?

They are references to the fact that the ssh daemon is ready to receive connections, one entry if for IPV4 the other for IPV6. (IPV4 are the familiar four byte (32 bit) addresses, IPV6 are new longer 128 bit addresses.

Any idea as to what the 0.0.0.0 is supposed to refer?

0.0.0.0 is a sort of network address wildcard. It means 'any IP address'

Please run

netstat –alt | grep ssh

What change to you see?

The port number 22 is now ssh and the host ip addresses have turned into hostnames.

Use the wc –l command to determin the number of lines in /etc/services. How many on your Centos machine.

11176 (may vary)

Next we run some commands to analyse the **layer 3** networking configuration.

Your machine is configured with both IPV4 addresses and IPV6. Run a command to show what they are.

ip address show

Ideally, we should not be using ifconfig!

Now show only IPV4 addresses

ip -4 a

Now IPV6

ip -6 a

Now show (all) the addresses configured on eth0

ip address show dev eth0

What is the (IPV4) netmask being used? How many bytes?

/24, three bytes (3)

How many octets are in the IPV6 subnet mask?

/64, eight bytes

Try the command

dig –t AAAA facebook.com

Are facebook using a vanity IP address?

Yes!

2a03:2880:f127:83:***face:b00c***:0:25de (or something similar)

Run the command to analyse the configuration file for the primary interface it uses (‘eth0’)

cat /etc/sysconfig/network-scripts/ifcfg-eth0

Look at the BOOTPROTO parameter, what is it set to?

dhcp

What can we say about how this server obtained an IP address, and what can we say about the network it is on?

It obtained its IP address from a DHCP service. Looking at the IPV4 IP address subnet mask (/24) , we know that the first three octets of its IP address represent the network it’s on, and that is possible to have up to 255 hosts on this network

Investigate which IP addresses are available on your network. Just get a rough idea. Start by pinging the servers of one or two other trainees on the course. For example, it seems that most of the IP addresses on the network are (or, perhaps, are *not*) in use

ping 10.0.0.1

… and so on

Almost certainly, most of the IP addresses on this network are not in use

Finally, we run some commands to analyse the **layer 2** networking configuration.

Below the network layer is the data link layer, which has attributes that are to do with your adapter card and Local Area Network set up. To view the Layer 2 attribute values run the command:

ip link show

Are these values also displayed using 'ip address show'? (Y/N)

Yes

One of the values for Layer 2 Maximum Transmission Unit (mtu), which determines the largest amount of data that can be encapsulated in a single Ethernet packet. What is the current value for the loopback (lo) interface?

65536 (this may vary)

Run the following command which simulates copying a large file to the server’s loopback interface

scp /var/log/messages root@localhost:/dev/null

Look at the speed of the transfer in MB/s. What is it? You could run this command four or five times and take the average

Approx 80MB/s (or somewhere in this region)

We will now set it to a lower value. Please run the command

ip link set mtu 150 dev lo

What does 'ip link show dev lo' reveal the mtu to now be?

150

Please run the scp command again. Does it go slower? What speed?

Yes, it goes a little slower, possibly less than 50MB/s, although this is by no means scientific, as there may be other traffic consecutively utilising this interface from time to time.

Please put mtu back!

ip link set mtu 65536 dev lo

Can you guess how you would make a permanent change to the MTU? Using the command is not persistent.

Add the line

MTU=xxxx to the ifcfg-lo file, in /etc/sysconfig/network-scripts.

Check you can connect using SSH to the loopback interface

ssh instructor@localhost

Exit out of that connection, and then take down the loopback interface, by running the following

ip link set down dev lo

Check this interface is down now

ip address show dev lo

Try connecting again using SSH to the loopback interface

ssh instructor@localhost

Cannot connect now

Bring that interface back up, check you can now connect against that interface

ip link set up dev lo

Yes, you can now connect to the loopback interface again