Basic IPv4 Configuration

This lab handout is intentionally kept brief so that students try to learn tools and commands in detail by themselves. The topics to be explored are:

1. Basic information on interfaces

   - Study interface naming conventions. When is interface named br0, xenbr0, virbr0, eth0, eth0:1, eth0.100, etc.

   - How can one identify which type of interface it is? For example whether it is ethernet interface, software bridge, aliases interface, etc. without deciding just based on interface name.

2. Learn about NetworkManager service. In particular:

   - What are advantages of using NetworkManager service

   - What are advantages of using network service

   - How to disable NetworkManager service

   - How to configure interface such that it is controlled by network service and not by NetworkManager service

3. Per-interface configuration file details. You should at least understand the purpose and usage of following parameters:

   - ONBOOT
   - NM_CONTROLLED
   - BOOTPROTO
   - DEVICE
   - HWADDR
   - IPADDR
   - NETMASK
   - BROADCAST
   - GATEWAY

   You should also explore other related problems / caveats related to ifcfg-* files like:

   - Changes to ifcfg-eth<n> file requires restarting network or ifup / ifdown for the particular interface for changes to take effect.

- If we delete the interface configuration file then interface can go down even without calling ifup / ifdown or restarting network explicitly.

- Lot of time people take backup of configuration file in same folder with appending '.bak' for indicating that it is backup. But initialization scripts load all ifcfg-* files on boot and hence even ifcfg-eth0.bak will get loaded and may interfere with configuration specified in ifcfg-eth0 file.

You are expected to explore more parameters and more caveats then just the ones listed here.

4. Learn information about iptables firewall. In particular:

- Why is firewall used?

- How to stop currently running iptables firewall?

- How to disable iptables firewall from running on start-up?

Note: You do not expected to learn how to configure iptables as part of this lab

5. Learn information about SELinux. In particular:

- What is SELinux? What are advantages of using SELinux?

- How to stop currently running SELinux?

- How to disable SELinux from running automatically on start-up?

Note: You are not expected to learn to configure SELinux contexts and solve SELinux related issues as part of this lab.

6. Learn about boot / service initialization scripts. In particular:

- What is use of '`service`' command?

- How is '`service`' command related to scripts in '`/etc/init.d`' folder?

- What is use of '`chkconfig`' command?

- How are links in '`/etc/rc.d/rc<n>.d`' folder related to '`chkconfig`' command?

- You should learn to use both '`service`' and '`chkconfig`' commands properly.

7. Learn to use 'ifconfig' command. In particular:

- Learn to use 'ifconfig' command to configure interface IP address and subnet-mask.

- Use it to see interface configuration details like currently configured IP address, netmask, MAC address, received packets, transmitted packets, received bytes, transmitted bytes, etc.

- Read 'man ifconfig' and learn other options like configuring interface MTU or putting interface in promiscuous mode.

Note: Do not spend time memorizing options supported by ifconfig command. You should just understand what are various parameters that can be configured using ifconfig and just remember to use ifconfig to set IP address / netmask. Other things can be done by referring to man page as and when required.

8. Learn to use 'tcpdump'. In particular:

- Various 'tcpdump' command line options.

- How to configure packet capture filters in 'tcpdump'.

- Saving packet capture in pcap files.

- Displaying information of packets stored in pcap file format.

Note: Do not spend time memorizing options supported by tcpdump command. You should just understand what are various options supported by tcpdump command so that you can use them as and when required.

This note applies to all commands being learned as part of course. You should only remember what each command is capable of and its most common used syntax / format. For rarely used options one can always refer to man page. There is no point trying to memorize rarely used options as eventually you would forget them after not using them for long time.

9. Learn to use 'wireshark'. In particular:

- Specifying packet capture filter in wireshark

- Specifying display filters in wireshark

- Use 'Follow TCP Stream' option in wireshark to see entire TCP stream to learn about protocols like HTTP, SMTP etc.

- Look at Layer / protocol wise displayed information about each field and parameter for each packet

- Look at various statistics calculated by wireshark.

- Use wireshark to save only selected packets / marked packets / displayed packets in another pcap file.

10. Learn to use ping to test network connectivity. Read 'man ping' to explore various options supported by ping command.

11. Study about ARP protocol and learn to use 'arp' command. In particular you should be able to:

  - See ARP table of machine
  - Add static ARP entries to ARP table

12. Try different subnet-mask / address configurations and observe effect on connectivity. For example for two machines in same LAN try following pairs of IP address and netmask combination and test connectivity between them. In each case you should understand why or why not machines are able to communicate with each other. IP address combinations to be tried are:

Machine I - IP address	Machine II - IP address
10.100.3.41/25	10.100.3.60/24
10.100.3.41/25	10.100.3.200/24
10.100.3.41/25	10.100.3.200/25
10.100.3.224/25	10.100.3.200/25
10.100.3.224/24	10.100.3.60/24

In each case also try to predict which of these machines machine I or machine II or both would be able to talk to gateway with address 10.100.3.1/24.

13. Learn to use 'ethtool' command. In particular:

  - Learn to configure auto-negotiation parameters.
  - Learn to disable auto-negotiation and configure duplex / speed manually. Try to connected two machines to a 100mbps switch through a 10mbps hub as shown below:

    Explain if any special configuration was required to make things work and why.
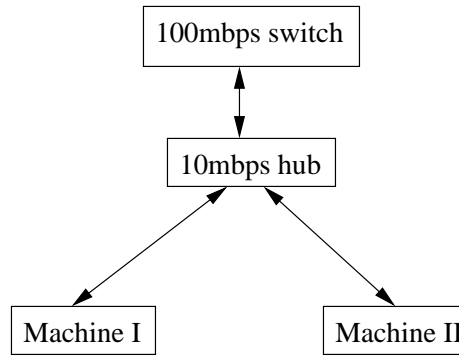
Figure 1: Connection to a 100mbps switch using 10mbps Hub in between

- Learn to enable disable checksum / fragmentation offload.
- Explore ETHTOOL_OPTS parameter for ifcfg-eth<n> configuration files

14. Compare performance of various switched networks (10 mbps vs. 100 mbps etc.) by transferring files, browsing websites, etc. and think about whether 10mbps is usable or at least 100mbps is required for normal useful work.

15. Compare 10mbps hub based network to 10mbps switch based network by transferring files, browsing websites, etc. Think and justify whether 10mbps hub based or 10mbps switch based or both are usable for normal useful work or not.

16. Study different types of cables, ports and connectors. In particular study about:

- Different types of ethernet cables
- Different types of fiber cables
- Different types of serial cables