Hands-on Projects

These projects should be completed in the order given. The hands-on projects presented in this chapter should take a total of three hours to complete. The requirements for this lab include:

* A computer with Fedora Linux installed according to Hands-on Project 2-1 and Ubuntu Server Linux installed according to Hands-On Project 6-1.

# Project 12-1

In this hands-on project, you view and modify the TCP/IP configuration of the network interface on your Fedora Linux and Ubuntu Server Linux virtual machines.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **ip a** which is short for address. At a minimum you should see two interfaces: lo which is short for loopback (every system with a network interface has a loopback referencing itself) and your interface that allows you out to the internet or local network.
   1. Record the name of the interface next to the number 2 (should start with enp but may be slightly different): **enp0s3**
      1. **You will now use this name in place of INTERFACE for the rest of 12-1.**
   2. Record the IPv4 address for the above interface (next to the inet value). **10.0.2.15/24**
      1. **You will now use this IP in place of interfaceIP for the rest of 12-1**
4. Display the contents of **/etc/sysconfig/network-scripts/ifcfg-INTERFACE** to your terminal. Review the output of your network interface configuration. Is your interface configured to be brought up upon system power-on? **Yes, the interface will boot on start up**
5. At the command prompt, type **ping interfaceIP** and press Enter. Do you receive ping responses from your network interface? **No, I’m not receiving ping responses**
6. At the command prompt, type **ip link set INTERFACE down** and press Enter. Next, type **ip a** at the command prompt and press Enter. Note that the state is DOWN.
7. At the command prompt, type **ping interfaceIP** and press Enter. Do you receive ping responses from your network interface? **No, I don’t receive ping responses**
8. At the command prompt, type **ip link set INTERFACE up** and press Enter. Now type **ip a** and review the state of the interface as UP.
9. At the command prompt, type **ping interfaceIP** and press Enter. Do you receive ping responses from your network interface? **No, ping responses** Press Ctrl+c when finished to quit the ping command.
10. At the command prompt, type **ip -s link** and press Enter. View the statistics for your network interfaces.
11. To be more specific, we can type **ip -s link show INTERFACE** to view the statistics for a specific interface.
12. Boot your Ubuntu Server Linux virtual machine. After your Linux system has been loaded, log into tty1 using the user name of root and the password of LNXrocks!.
13. At the command prompt, type **ip a** and press Enter. What IPv4 and IPv6 configuration do you see for eth0?
14. Display the contents of **/etc/network/interfaces** to the terminal. Is IP information obtained automatically for eth0? What lines could you modify and add to this file to set a static IP configuration? **Yes it is obtained automatically.**
15. At the command prompt, type **ip link set eth0 down ; ip link set eth0 up** and press Enter.
16. **Provide screenshot(s) of steps 3 through 15.**

# Project 12-2

In this hands-on project, you view your host name as well as resolve host names and configure host name resolution.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **hostname** and press Enter. What is your host name? **clopez13.iit.edu**
4. Display the contents of **/etc/hostname** to the terminal. What host name is listed here? **Clopez13.iit.edu**
5. Display the contents of **/etc/resolv.conf** to the terminal. Review the nameservers that you will use to resolve DNS names to IP addresses.
6. View the **/etc/nsswitch.conf** file and find the portion referencing hosts. This file is used by the GNU C Library to determine the sources from which to obtain name-service information and the order to obtain them. Will files such as /etc/hosts be used for name resolution before DNS? Why? **Yes, because it references myhostname**
7. **Edit** the /etc/hosts file with a text editor such as vim. Add a line to the bottom of the file that reads:

InterfaceIP fakehost.fakedomain.com sample

When finished, save your changes and quit the editor.

1. At the command prompt, type **ping -c 5 localhost** and press Enter. Was the name resolved correctly? **Yes, it was resolved correctly**
2. At the command prompt, type **ping -c 5 fakehost.fakedomain.com** and press Enter. Was the name resolved correctly? Was the ping command able to contact the host? **No, it was not resolved correctly. The ping command failed**
3. At the command prompt, type **ping -c 5 sample** and press Enter. Was the name resolved correctly? Was the ping command able to contact the host?  **No, the name was not resolved correctly and the ping never started**
4. On your Ubuntu Server Linux virtual machine, log into tty1 using the user name of root and the password of LNXrocks!. Perform Steps 2 through 9 and note any differences. **3.)clopez13; 4.)clopez13; 6.)yes, it comes first in the order before dns; 8.) yes, it was resolved correctly; 9.) no, it was not resolved correctly and the ping command failed; 10.) no, the name wasn’t resolved correctly and the ping never started**
5. **Provide screenshot(s) of steps 3 through 11 for both Fedora and Ubuntu.**

# Project 12-3

In this hands-on project, you test name resolution using your ISP’s DNS server on your Ubuntu Server Linux virtual machine.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **host kernel.org** and press Enter. What IP address was returned for kernel.org? What is the hostname for their mailserver? **198.145.29.83; 10 mail.kernel.org**
4. At the command prompt, type **nslookup kernel.org** and press Enter. What DNS server was used to query this information? Why? **216.47.143.106, because that’s the address of kernel.org**
5. At the command prompt, type the command **dig kernel.org** and press Enter. What DNS record did we request? What was the value of the record? Why? **216.47.143.106**
6. At the command prompt, type the command **dig kernel.org MX** and press Enter. What is the value of the MX record? Does this match the output provided in step 5? **216.47.143.106, yes it does**
7. **Provide screenshot(s) of steps 3 through 6.**

# Project 12-4

In this hands-on project, you view and configure the route table on your Fedora Linux virtual machine as well as view and test your routing configuration.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **ip route** and press Enter. What IPv4 address is listed as your default gateway? What interface is this reachable IP reachable from? **10.0.2.0/24; enp0s3**
4. At the command prompt, type **traceroute kernel.org** and press Enter. This may only show 2 hosts depending on how networking is configured at the VM level. The default protocol for Linux based traceroute is ti use UDP.
5. At the command prompt, type **traceroute -I kernel.org** and press Enter to utilize ICMP rather than UDP. How many hops are displayed? Do any show \* if so why? **There are 17 hops. Since there is a record of each hop and the destination is reached.**
6. At the command prompt, type **ip route add IP\_OF\_KERNELORG via 127.0.0.1** and press Enter, *where IP\_OF\_KERNELORG is the IPv4 address resolved from project 12-3*. We have now created a null route. When we attempt to go to the IP address of kernel.org, we will be routed to our loopback address rather than out to our default gateway.
7. At the command prompt, type **ip route** and press Enter. Is the route added visible? **Yes, it is visible**
8. At the command prompt, type **traceroute -I kernel.org** and press Enter. Notice that we have all \*\*\* for the entries displayed. This is due to the null route we created above. Why does traceroute stop at 30 hops? **Beacause that is the limit of how many stops to make before there is no stops made**
9. At the command prompt, type **ip route del IP\_OF\_KERNELORG** and press Enter. We can again access kerel.org
10. At the command prompt, type the command **cat /proc/sys/net/ipv4/ip\_forward** and press Enter. Is your system configured as an IPv4 router? **Yes** Next, type **cat /proc/sys/net/ipv6/conf/all/forwarding** and press Enter. Is your system configured as an IPv6 router? **No**
11. **Provide screenshot(s) of steps 3 through 10.**

# Project 12-5

In this hands-on project, you utilize the SSH remote access utility.

1. Boot your **Fedora** Linux virtual machine. Login to your chosen desktop environment as **user1** using password **LNXrocks!** and open up a terminal window.
2. At the terminal, become **root** by typing **su -** and press enter and provide **LNXrocks!** as the password.
3. At the command prompt, type **systemctl status sshd.service** and press Enter to see if the SSH daemon started at boot time. If not, start the sshd.service.
4. At the command prompt, type **ssh user1@localhost** and press Enter. When prompted to connect to the remote system, type yes and press Enter. Next, supply the user’s password of LNXrocks! and press Enter.
5. At the command prompt, type **who** and press Enter. Type **exit** and press Enter to log out of your remote shell.
6. At the command prompt, type **ssh -X user1@localhost** and press Enter. Supply the user’s password of LNXrocks! and press Enter when prompted.
7. At the command prompt, type **gnome-calculator** and press Enter. Note that this command starts the calculator software forwarded over your SSH session. This could be done with another system across the network rather than our local system in the example.
8. At the command prompt, type **ssh student@64.131.110.40** and accept the RSA fingerprint and supply the students password of LNXrocks! when prompted. You are now logged into the class server.
9. Notice when you login, you are prompted with a banner showing some information regarding the system. Where is this file located? What is the name of the file? (hint chapter 7 global environment files). What two commands create the cow speaking when we log in? **~/.ssh/known\_hosts; ECDSA key;**
10. At the command prompt, type **sl** and press enter. Enjoy.
11. At the command prompt, type **w** and press Enter to see if anyone else is logged into the server. Type **exit** and press Enter to log out of your remote shell.
12. At the command prompt, type **ssh student@64.131.110.40 cat /etc/system-release > server\_version** and supply the students password of LNXrocks! when prompted.
13. Review the **server\_version** file we created in your current directory. What OS and version is the server running? **CentOS Linux 7.3.1611**
14. At the command prompt, type **scp student@64.131.110.40:/etc/os-release .** Enter to copy the /etc/os-release file from the class server to your current directory on your Fedora system. Supply the students password of LNXrocks!
15. Display the contents of the **os-release** file to the terminal.
16. Review the **/etc/ssh/ssh\_config** file. Examine the SSH client options available. Note the encryption algorithms supported in the commented Ciphers line. What are the ciphers provided in this file? **Aes128, aes192-ctr, aes256-ctr, arcfour256, arcfour128, aes128-cbc,3des-cbc**
17. Review the **/etc/ssh/sshd\_config** file. Examine the SSH daemon options available. What line would allow root connections to the SSH daemon if they were not allowed by default?
18. Review the **/root/.ssh/known\_hosts** file. What two hosts are listed in this file and why?
19. **Provide screenshot(s) of steps 3 through 18.**