CIT 371 lab 20: Network Configuration

This lab can be done with SSH/PuTTY or with the Web Console. See the Student VM Access document for information on accessing your VMs.

Read chapter 12 before doing this lab. su to root for the entire lab.

1. Test the following services: *which of these are running?* certmonger, firewalld, network, NetworkManager, ntpd. *Of these services, which are critical to being able to communicate over the network? Which are there for security purposes?*
   1. **The following that are running are firewalld, network, and NetworkManager. The services that are able to communicate over the network are NetworkManager and network. The firewalld is for security purposes.**
2. We will now examine your interfaces and what they do. Type **ip addr** to obtain your IPv4 address (listed under ens33 as inet). There will also be an IPv4 address for your loopback device (127.0.0.1). Ignore the IPv6 addresses and those of virbr0 and virbr0-nic.
   1. Type **systemctl stop network**. Ping your ens33 address. *What happens?* Ping your lo address. *What happens?* Restart your network service, retry the ping commands for eth0 and lo. *What happens?* Use systemctl to stop NetworkManager. Repeat the two ping commands. *What happens?* Restart NetworkManager. NetworkManager is the more important than network, but *which is needed for ping to work?* Let’s see why. Stop the network service and type **ip addr**. You still have IPv4 addresses for lo, virbr0 and virbr0-nic but not ens33. *What does this mean?* Restart network, *did you regain your IPv4 address for ens33?* Stop NetworkManager and repeat **ip addr**. Restart NetworkManager. *Summarize what happens with your Ethernet card’s IPv4 address when stopping network vs NetworkManager.*
      1. **The network is unreachable. The network still seems to be unreachable. This still allows us to ping. Network is needed for the ping to work. This means that the network seems to not be assigned to our ens32. Yes, we regained our IPv4 address again. Since we are stopping the network card this means we are disconnected from the internet but this doesn’t disconnect you from your IP address.**
   2. Type **cd /etc/sysconfig/network-scripts**. Examine both files ifcfg-ens33 and ifcfg-lo. These are configuration files for your interfaces: Ethernet card (ens33) and loopback (lo). lo’s IPv4 address is hardcoded into its file, ens33’s is not. Ens33 gets its IPv4 address using DHCP (see the entry BOOTPROTO=“dhcp”). With ONBOOT=“yes”, your Ethernet card obtains its IPv4 address upon booting (and whenever the network service starts). The IP address for lo never changes (127.0.0.1). Copy ifcfg-ens33 to ifcfg-ens-temp. Now, edit **ifcfg-ens33** in vi, changing BOOTPROTO to “static”, adding two lines: **IPADDR=…** where **…** is your IP address as obtained from step 2a and **NETMASK=255.255.224.0**. **Save** the file, restart your **network** service. Ping your IPv4 address. *What happens?*  You have the same IP address so nothing changes. This is risky though because a DHCP server cannot guarantee you the same address each time you request one and if it has assigned this address to someone else, we can have problems and if you make a mistake, it could leave you without Internet access. Re-edit this file and change the IP address to **1.2.3.4**. Save the file and restart network. Type **ping 1.2.3.4**. *What happens?* Try to ping www.nku.edu. *What happens?* Your messages are able to make it to the network, but the router does not know your new address to route messages back to you! Move ifcfg-ens-temp back to ifcfg-ens to return it to its original value form. Restart the network service.
      1. **The ping is transmitted and runs itself. When we try to ping 1.2.3.4. we are able unable to and says destination host unreachable. When we ping** [**www.nku.edu**](http://www.nku.edu) **this works and transmits the ping.**
   3. Type **ls** in the network-scripts directory. There are several script files (green font) and symbolic links. The links link to services that control your interfaces. We are interested in two, ifup and ifdown. Type **./ifdown lo**. Type **ip addr**. *What does the state say for lo?* Bring it back up using **./ifup lo**. Repeat **ip addr**. *What is lo’s state now?* 
      1. **State says that it is DOWN. Lo’s state now is UNKOWN.**
   4. Bring down your Ethernet interface. *What command did you enter? What message did you receive?* As an experiment, ping your ens33 IP address (from step 2a). *Are you able to ping either? Why do you suppose you got the result you got?* Bring your Ethernet back up. *What command did you enter?* Repeat the ip addr and ping commands.
      1. **./ifdown ens32 . The message received was “ device ens32 successfully disconnected”. You are unable to connect to the network, network is unreachable. I suppose we got the results because we shut down the network making it unable to reach or ping the connection. ./ifup ens32**
3. To wrap up this lab, we will examine how your interfaces communicate with your network.
   1. Your computer communicates with a network switch, which keeps track of your interface by *hardware (MAC) address*. Type **ip addr** and look at the ens33 entry link/ether. *What is your interface’s address?* Your IPv4 address might change over time but the MAC address should never change. The network switch communicates with routers to translates MAC addresses to IP addresses using a protocol called ARP. Type **ip route** which gives you information about the router that links you to the rest of our network. The first line says “default via” followed by an IP address, which is your router’s IP address. *What is it?* Ping it. Type **traceroute www.nku.edu**. The first entry is this router. Type **traceroute www.uc.edu** and you will find the same first entry. Return to the ip route output. The first line tells you that you connect to the router via ens33. proto indicates how the route was established (other values are redirect (installed by a redirection from another device), kernel (installed during kernel autoconfiguration), boot (installed during the bootup sequence), static (installed by hand), ra (discovered using the Router Discovery Protocol)). *Which does it say for your entry?* Metric indicates a preference of which router to use (this is important when there are multiple routers, the lower metric router is selected first, other routers are tried only if this router fails). *What value is specified?* The next line starts with your network address in prefix form. The number after the / indicates the number of consecutive 1s at the begining of the netmask (10.2.6.0/24 has a netmask of 11111111.11111111.11111111.00000000 or 255.255.255.0). Given that first #, determine your netmask in binary and then convert it into decimal. *Place your netmask, in decimal, in your answers.* The next line contains an IP address of a DNS name server for the domain. The statement proto dhcp indicates that you obtained this address when you requested an IP address from your DHCP server. Type **dig –x *ipaddress*** using the IP address at the start of this line to obtain this name server’s name. *What is it?*
      1. **My interfaces address is 00:50:56:b9:70:fb . My router IP address is 10.2.56.1 . My entry says proto dhcp. Metric 100. My netmask in decimal form is 11111111.11111111.11111.10.2.65.0 . DiG 9.9.4-RedHat-9.9.4-61.e17 .**
   2. Type **ip route show table local** to view your entire routing table. This table becomes populated as you use your network. Entries may become stale (outdated) so we might flush the table. Type **ip route flush table local**. Repeat the show command. *What has happened to the entries in your table?* Type **ping www.nku.edu**. *What happens?* Since your routing table is empty, your computer does not know who to contact to send out messages. Restart your network service (**systemctl restart NetworkManager**). Repeat the show and ping commands. *Do you have your router information back? Did ping work successfully?*
      1. **All the entries in the table have disappeared. The ping is unable to ping. Yes we have router information back and the ping was successful.**
   3. Type **ip neigh show**. This displays ARP information. *What does ARP stand for?* The listing from this command shows information from the ARP table. Your router’s IP address is listed here and should be REACHABLE. Flush the ARP table (like you flushed the router table in 3b) using **ip neigh flush *ipaddress*** where *ipaddress* is the address of your switch/router/gateway. Repeat the show command. *What is its state now (as opposed to REACHABLE)?* Type **ping www.nku.edu**. You might be surprised to see this work. Exit out of ping, repeat the show command. The information is restored. Why? Ping sends out a packet on the network looking for any connection and your switch receives it and responds, having stored your MAC address back in its ARP table. That is, using the network automatically resources the ARP table, unlike what happened in step 3d where flushing the router table required a different operation to repopulate it.  *In summary, explain what ARP does and compare what a switch operates on versus a router.*
      1. **ARP stands for address resolution protocol. The state now is unreachable, and the information has been removed. ARP is a communication protocol used for discovering the link layer address, such as a MAC address. This is usually associated with a given internet layer address, such as our IPv4 address. A switch connects multiple devices to create a network, while as a router connects multiple switches**

Shut down your VM if desired, disconnect from the VPN if you are using it, and submit your lab report.