Networking - CentOS

Prerequisites for the script on CentOS: There are a few prerequisite packages that may need to be installed for this script to function correctly. Use the following commands to install them.

Speedtest-cli

The speedtest-cli package is required to run the speedtest-cli command to test your network upload and download speed. Run the following command to install the it.

sudo yum install speedtest-cli

Traceroute

You may need to install traceroute if it is not already installed. First, verify if traceroute is installed using the following command.

which traceroute

If traceroute is not found and needs to be installed, run the following command.

yum install traceroute -y

Nslookup

You will also need to have nslookup installed. If the command is not found, use the following command to install bind-utils package which includes the nslookup command.

yum install bind-utils

Ping

If you are currently unable to use the ping command, you will need to install iputils. Use the following command to install the iputils package to get the ping command functioning.

yum install iputils

TCPdump

If the TCPdump command is not installed, you can install it using the command provided below.

yum install tcpdump

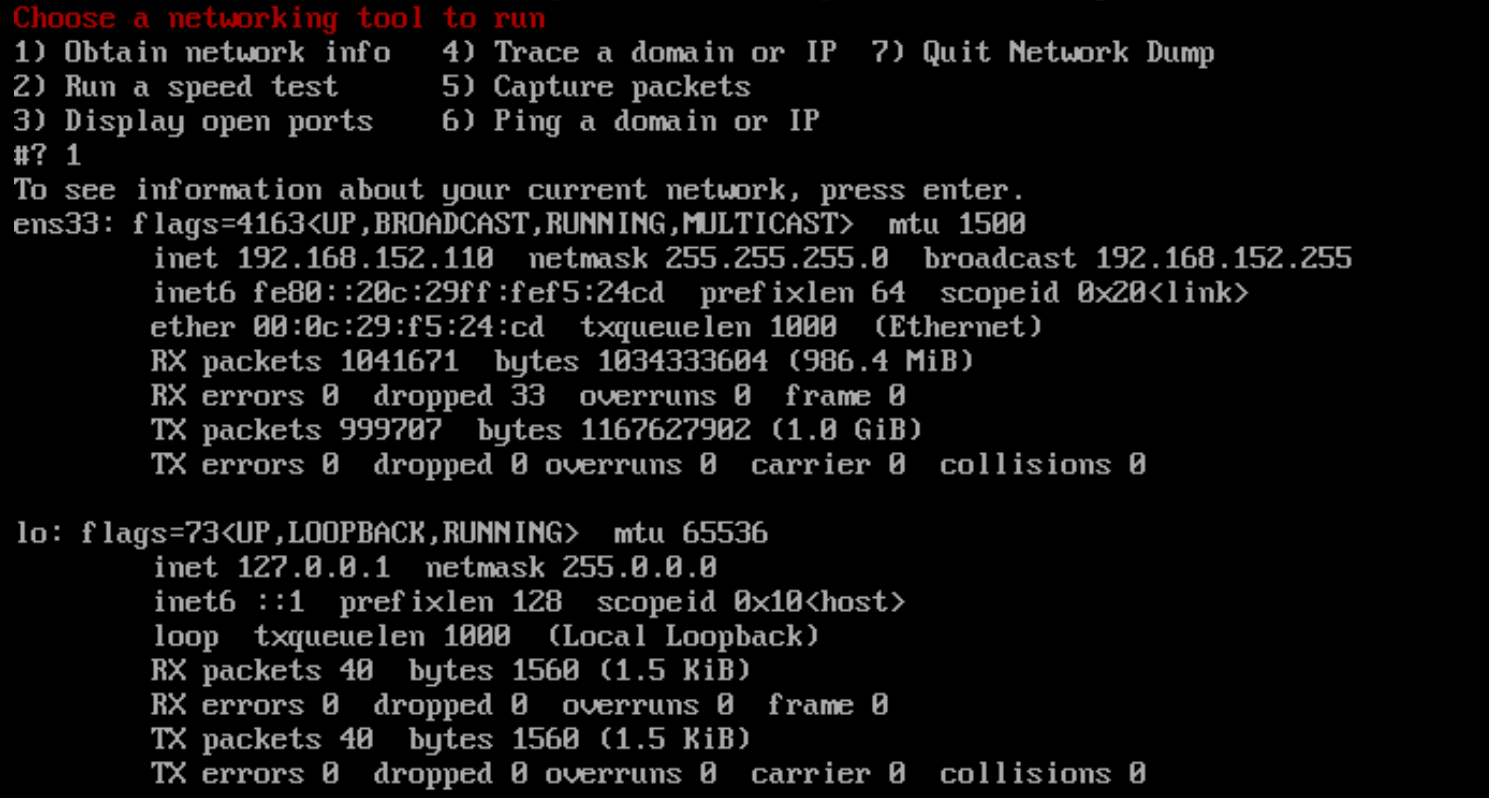
Using the script: To run the script, change directories to where the script is downloaded. Then use chmod +x to make the script executable.



After this, you can run this script using ./network-dump.sh You then will see a menu displaying different networking programs that you can run. After you run a network tool, the results are dumped to file called NetworkDump\_(current date) in the active directory. You will return back to the menu after each tool. Use 7 “Quit Network Dump” to quit running the script.

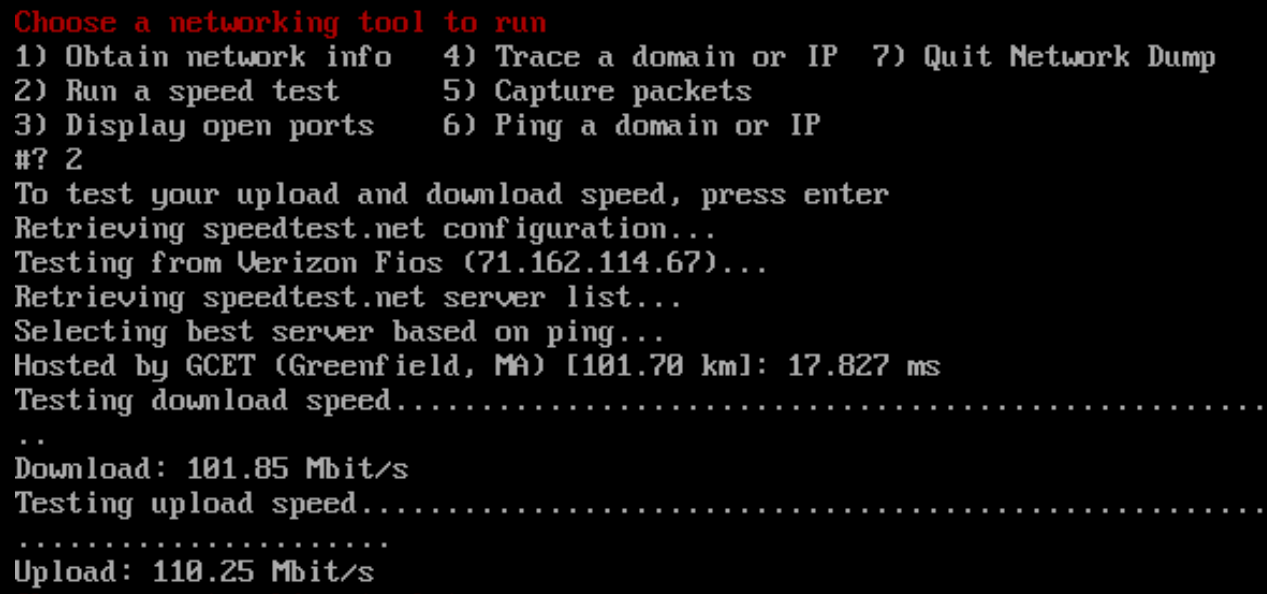


1. Obtain network info: The first option available is “Obtain network info”. To access this, type 1 and press enter. You should now see a prompt saying "To see information about your current network, press enter.". Press enter and you should see information about your current network adapters.



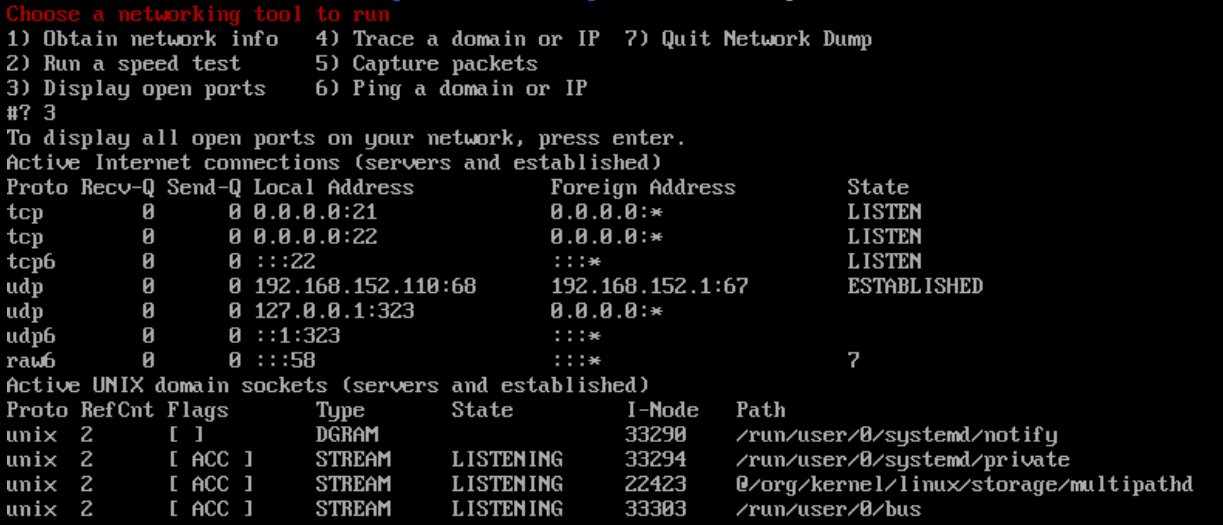
This program uses the command ifconfig -a to display all network interfaces available. This could be useful in a networking environment to find out which network devices are enabled and disabled on a machine.

1. Run a speed test: The second option available is “Run a speed test”. To access this tool, type 2 and press enter. You should now see a prompt saying "To test your upload and download speed, press enter". Press enter and you will see your download speed and upload speed being tested using the servers from speedtest.net. At the bottom you will see the results of the speed test. In this screenshot my download speed is 101.85 Mbit/s and my upload speed is 110.25 Mbit/s.



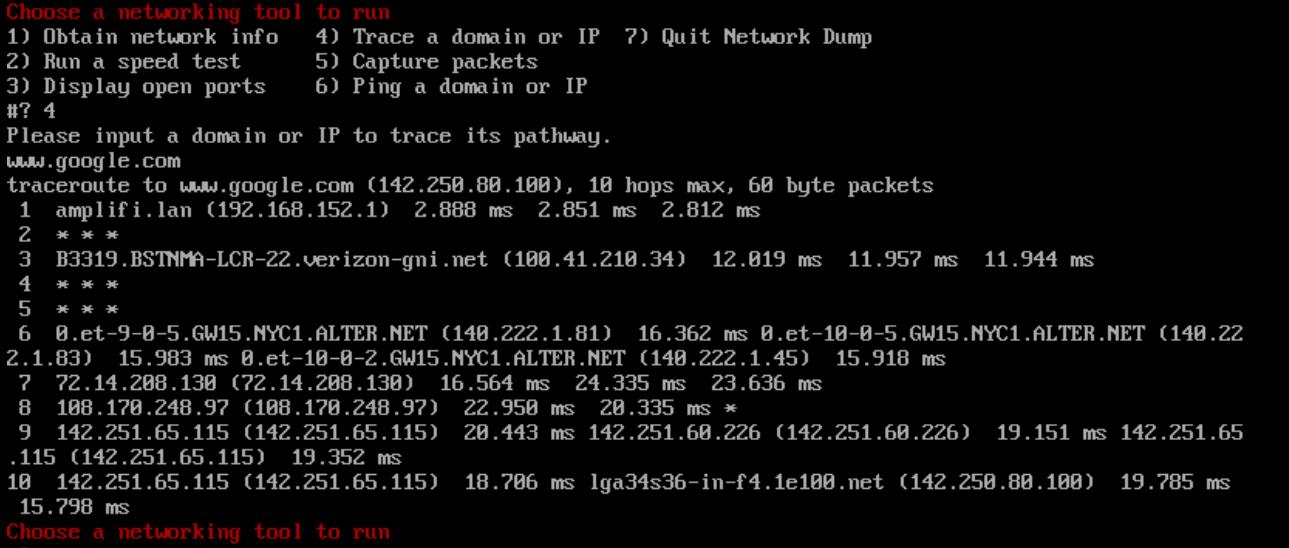
This program uses the command speedtest-cli to test the performance of your current network’s upload and download speed. It fetches the most optimized server available from speedtest.net and then downloads and uploads a small test file. After this, you can observe the resulting speeds. This could be useful in a networking environment to test the speed of your current network.

1. Display open ports: The third option available is “Display open ports”. To access this tool, type 3 and press enter. You should now see a prompt saying “To display all open ports on your network, press enter”. Press enter and you will then see a list of all open ports within your network. This table is organized by protocol (TCP or UDP), IP address, and current state.



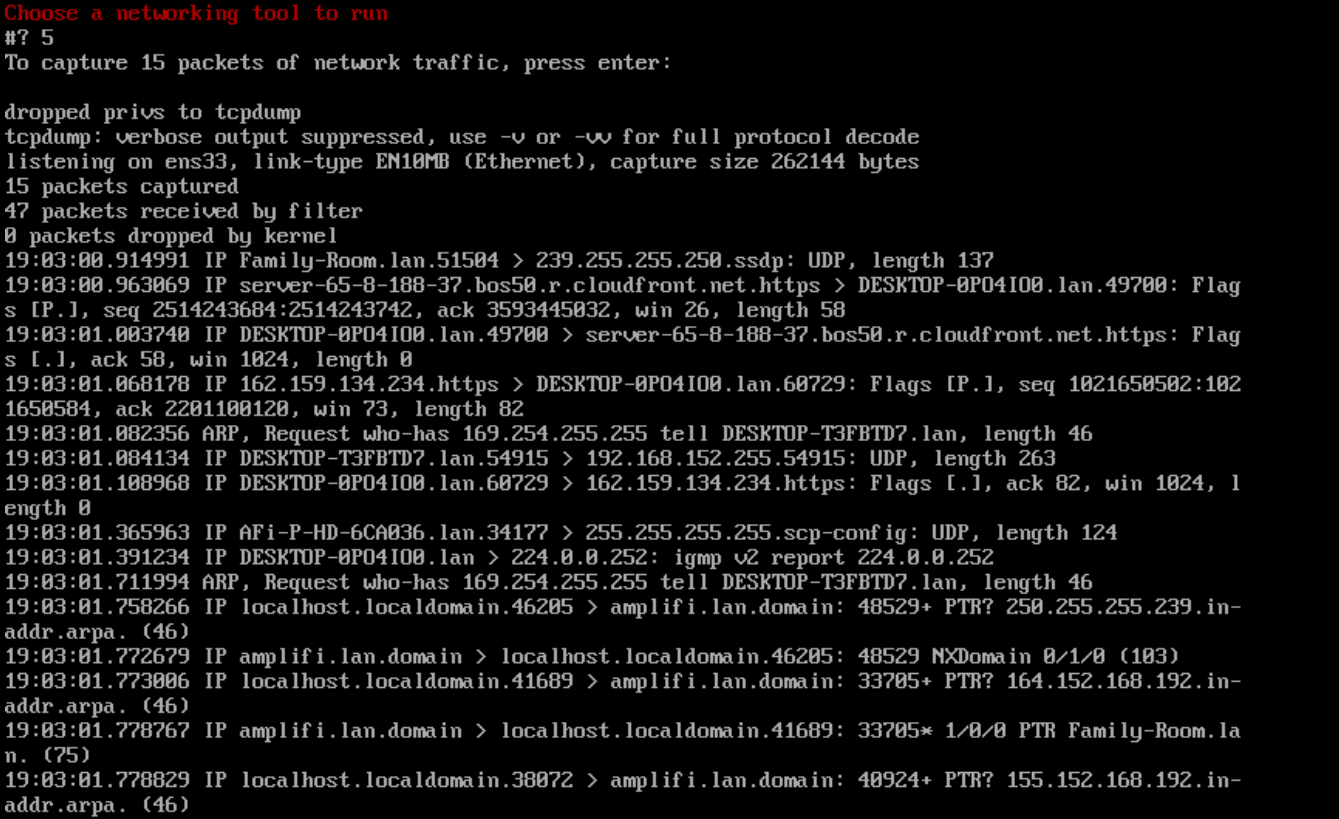
This program uses the netstat command which displays all of the active TCP connections and TCP and UDP ports of which the device is listening. I also used the additional parameters -a which displays all active ports and -n which adds a numerical display of the addresses and port numbers. This tool is useful to secure a network by identifying and closing unused ports.

1. Trace a domain or IP: The fourth option available is “Trace a domain or IP”. To access this tool, type 4 and press enter. You will now need to input a domain or IP you would like to test for the traceroute. This tool is useful to determine if a network has delayed responses during in a network path.



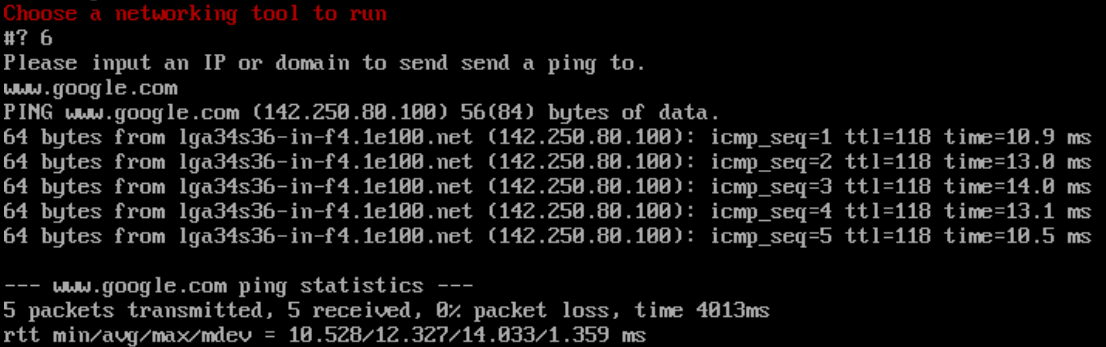
This program uses the command traceroute and takes an input from the user to trace the path of data packets from and to the domain or IP provided over 10 hops. It uses the parameters -m 10 to specify that the there can only be a maximum of 10 hops before the commands completes.

1. Capture Packets: The third option available is “Capture packets”. To access this tool, type 5 and press enter. You will then see a message saying “To capture 15 packets of network traffic, press enter”. Press enter and you will then see a list displayed of the last 15 packets transferred between your network connection.



This program uses the command tcpdump to capture network packets that are being transferred through your system. I also used the additional parameter -c 15 to limit the capture to a total of 15 packets. This is to prevent and endless or exaggerated amount of packet captured. The tcpdump tool can be useful to analyze network traffic of your system and can also be used with many filters or configurations.

1. Ping a domain or IP: The next option available is “Ping a domain or IP”. To access this tool, type 6 and press ender. You will then be asked to input a domain or IP in which you want to ping. After, press enter and you will see the tool perform a ping test to the IP. The ping tool is commonly used in many networking environments to quickly identify issues with your network configuration or a server.



This program uses the command ping to send packets of data to a user input domain or IP. The packets are then sent back and the response time is recorded in the results. It also uses the parameter -c 5 to limit only 5 pings sent. The parameter -t can also be used to constantly ping a domain or IP. This command is very useful for testing whether your system can effectively communicate with systems on your own network or connect to web domains.

1. Quit network dump: The final option provided is “Quit network dump”. This is provided if you would like to stop using the script. To quit, type 7 and press enter. The script is now closed.