THE UNIVERSITY OF TENNESSEE CHATTANOOGA

Using Terminal Commands in the Network

Mckenzie Mack
GenCyber Workshop

Agenda

- Examining Your Network
- Commands to Use
- Other Uses

Learning Objectives

- Explain how commands are used to communicate and identify nodes on the network
- Show use of ifconfig, ping, and other commands
- Describe why the commands discussed are valuable for network analysis and diagnosis

Examining Your Network

- Earlier you learned what a network is and how communication occurs across a network
- How do you find out more information about your own network?
  - the source address of your device?
  - another node’s destination address?
  - a packet’s path across the network?

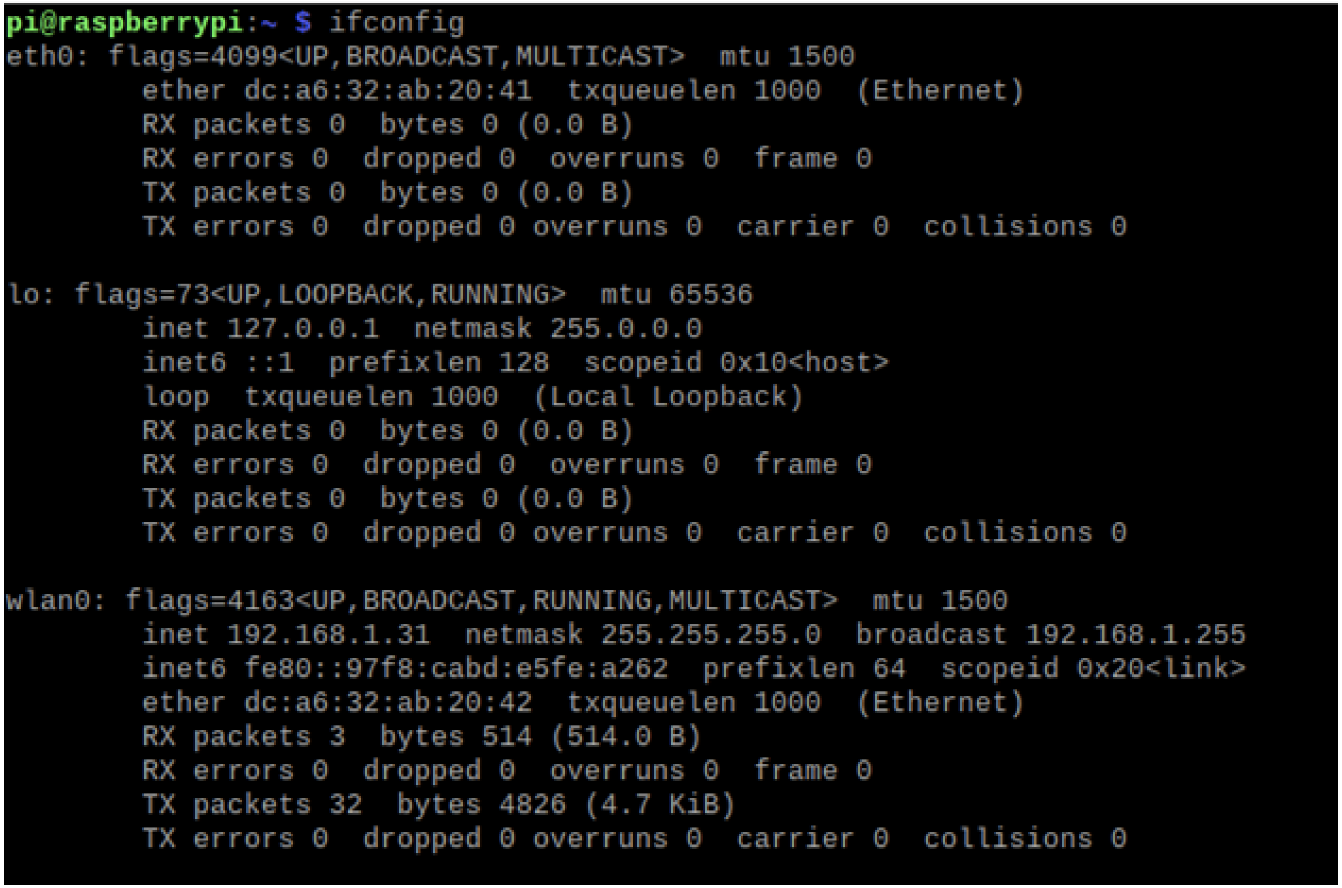
Examining Your Network

- One way to find this data is to use commands that retrieve this information through a command-line interface (CLI)
- Some of these commands include:
  - ifconfig
  - iwconfig
  - ping
  - traceroute

Commands to Use

- ifconfig
  - used to configure a **network interface**
    - network interface: point of connection between your computer and the network
  - can be used to set an IP address, set a subnet mask, etc.
  - also used to view information in an existing network interface
    - inet = your device's IP address
    - netmask = subnet mask
    - broadcast = the network's broadcast address (used to broadcast a message to all devices on a network)
    - RX packets = number of received packets
    - TX packets = number of transmitted packets

Commands to Use

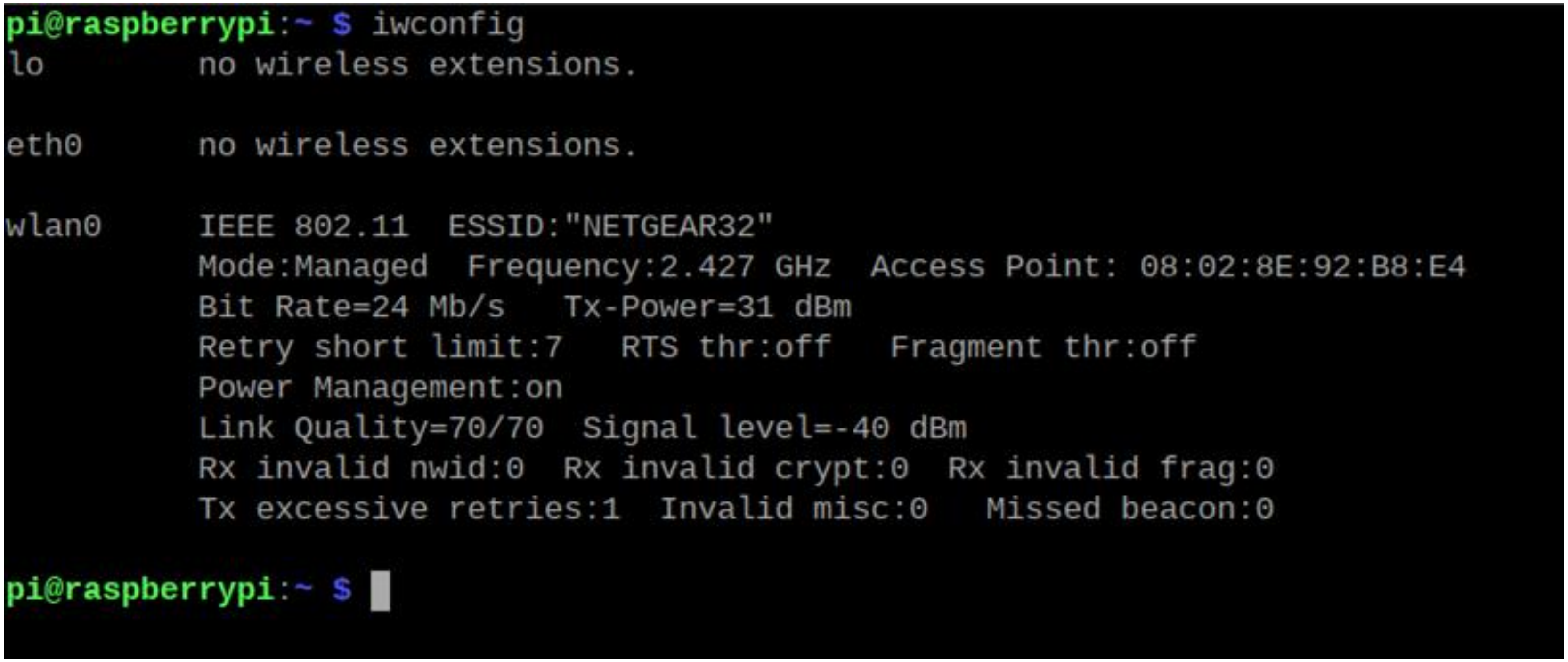


```
pi@raspberrypi:~ $ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether dc:a6:32:ab:20:41  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.31  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::97f8:cabd:e5fe:a262  prefixlen 64  scopeid 0x20<link>
        ether dc:a6:32:ab:20:42  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 514 (514.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 4826 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Commands to Use

- If you wanted to find out more about your wireless connection specifically, you could use **iwconfig**
  - could also be used to modify your wireless network interface
  - iwconfig displays:
    - the name of the network
    - the frequency of the channel that you are operating on
    - the bit rate of your connection, etc.

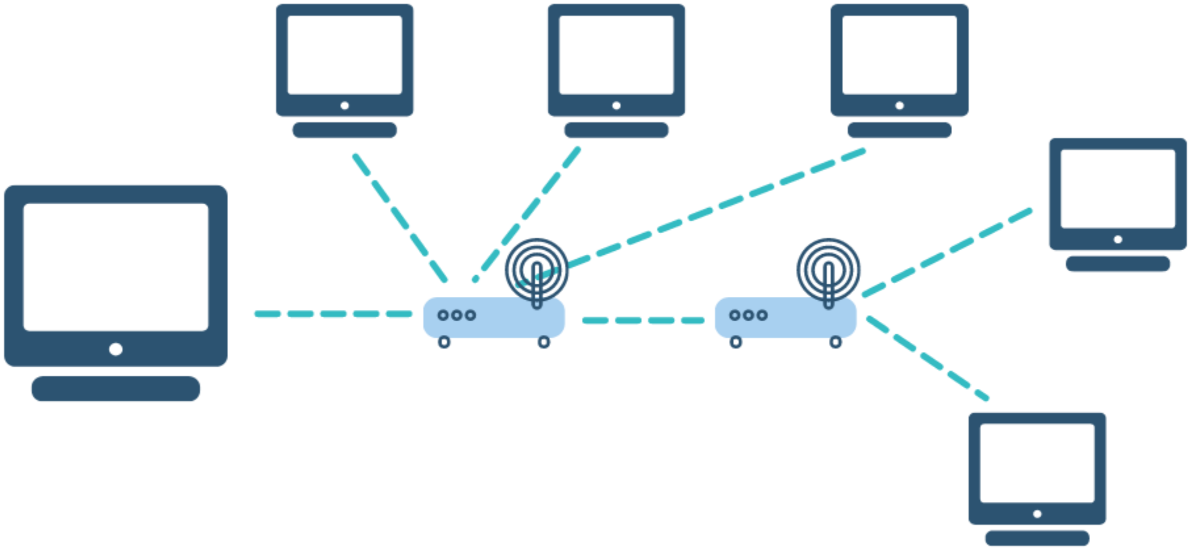
Commands to Use



```
pi@raspberrypi:~ $ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"NETGEAR32"
          Mode:Managed  Frequency:2.427 GHz  Access Point: 08:02:8E:92:B8:E4
          Bit Rate=24 Mb/s   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70  Signal level=-40 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1  Invalid misc:0   Missed beacon:0

pi@raspberrypi:~ $ 
```

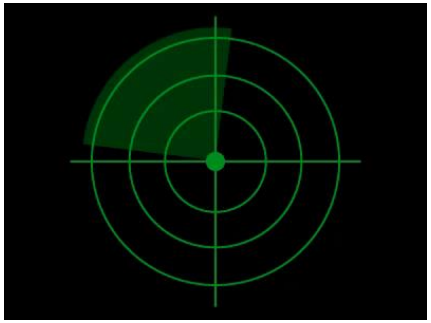
Commands to Use

- Now that you know more about the network in terms of your own device, let’s explore some commands that tell your more about other devices (also known as **nodes**) on the network



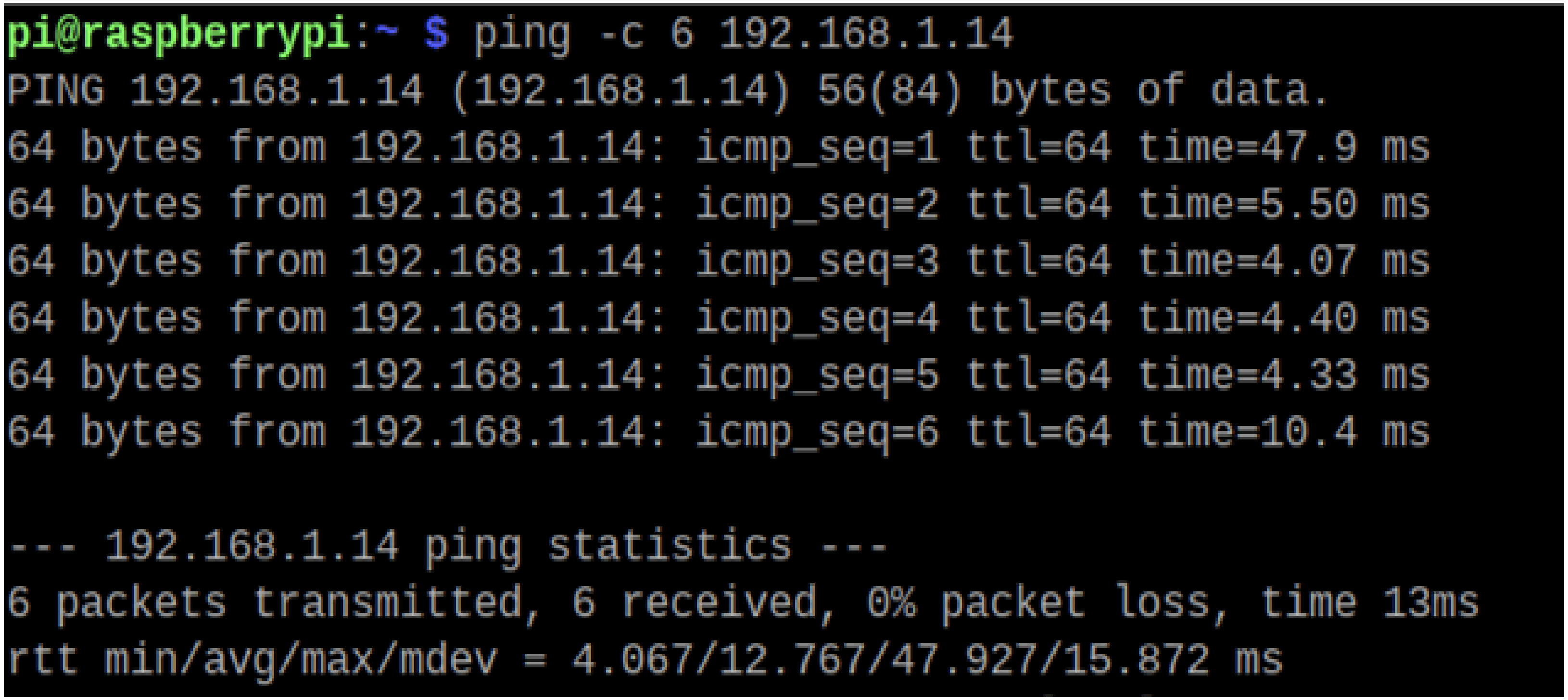
Commands to Use:

- ping:
  - used to test the connectivity between your device and another device on the network
  - the command sends a series of packets to the other device and waits for a reply
  - calculates the round-trip time (rtt) for each packet
  - displays the time-to-live (ttl) of each packet
  - tells you if any packets were lost
- **-c x** where **x** is a number specifies the number of packets to be sent by the command (ex: if you typed **ping -c 4**, 4 packets would be sent to the destination address)



Commands to Use

- in order to use ping, **you must know the other device's IP address**



```
pi@raspberrypi:~ $ ping -c 6 192.168.1.14
PING 192.168.1.14 (192.168.1.14) 56(84) bytes of data.
64 bytes from 192.168.1.14: icmp_seq=1 ttl=64 time=47.9 ms
64 bytes from 192.168.1.14: icmp_seq=2 ttl=64 time=5.50 ms
64 bytes from 192.168.1.14: icmp_seq=3 ttl=64 time=4.07 ms
64 bytes from 192.168.1.14: icmp_seq=4 ttl=64 time=4.40 ms
64 bytes from 192.168.1.14: icmp_seq=5 ttl=64 time=4.33 ms
64 bytes from 192.168.1.14: icmp_seq=6 ttl=64 time=10.4 ms

--- 192.168.1.14 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 4.067/12.767/47.927/15.872 ms
```

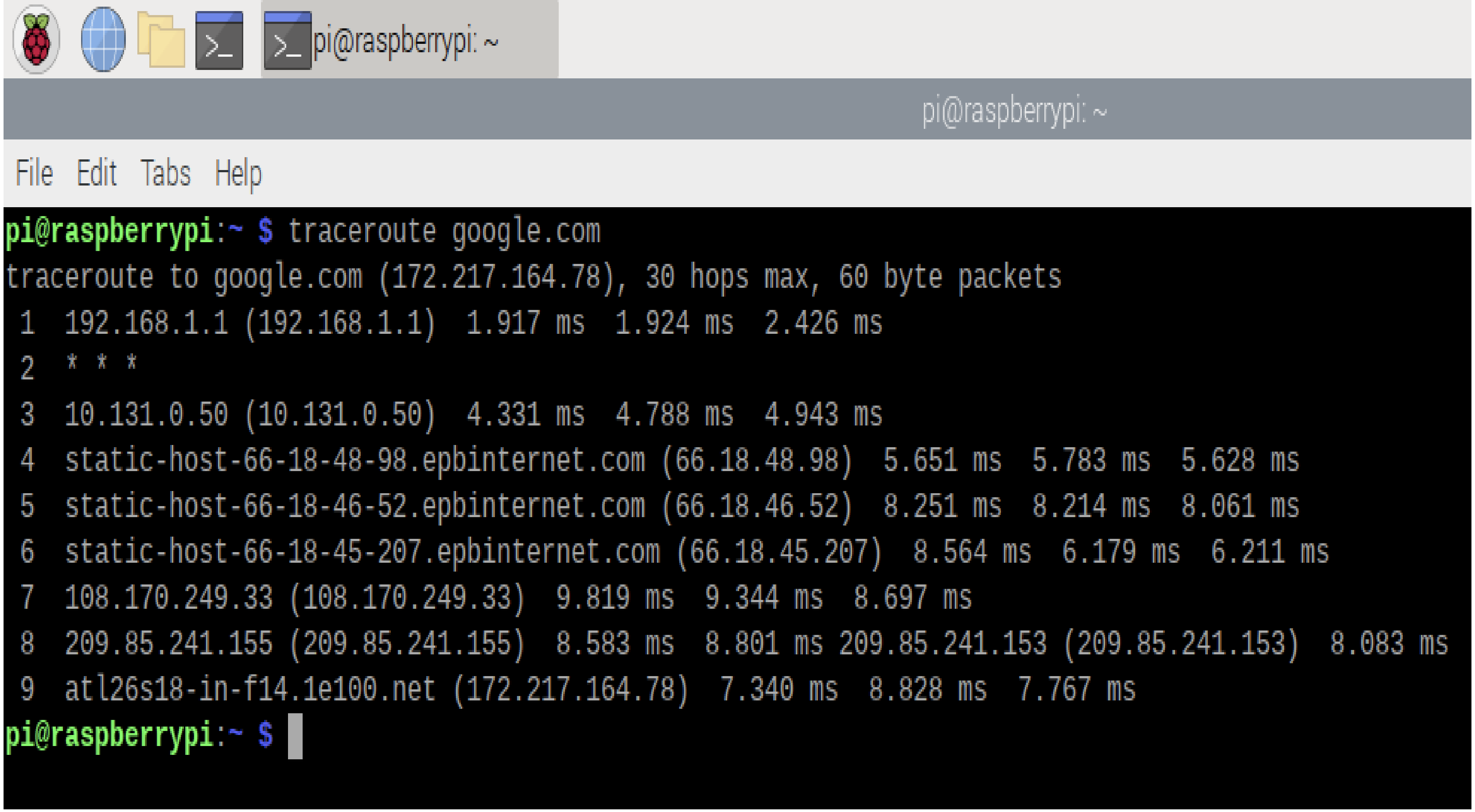
Commands to Use

- traceroute
  - similar to ping, but displays information about each hop on the route
    - think of when you track a package being delivered to your house
  - lists each intermediate device’s name (if known) and IP address

Commands to Use

- for each intermediate device, traceroute forces the device to drop a packet and send an error message back to the source
  - traceroute then uses this error message to calculate the rtt of each “hop”
  - calculates rtt three times for each intermediate device
- *** indicates that a reply from the router was not received within a certain time frame

Commands to Use



```
pi@raspberrypi:~ $ traceroute google.com
traceroute to google.com (172.217.164.78), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  1.917 ms  1.924 ms  2.426 ms
 2  * * *
 3  10.131.0.50 (10.131.0.50)  4.331 ms  4.788 ms  4.943 ms
 4  static-host-66-18-48-98.epbinternet.com (66.18.48.98)  5.651 ms  5.783 ms  5.628 ms
 5  static-host-66-18-46-52.epbinternet.com (66.18.46.52)  8.251 ms  8.214 ms  8.061 ms
 6  static-host-66-18-45-207.epbinternet.com (66.18.45.207)  8.564 ms  6.179 ms  6.211 ms
 7  108.170.249.33 (108.170.249.33)  9.819 ms  9.344 ms  8.697 ms
 8  209.85.241.155 (209.85.241.155)  8.583 ms  8.801 ms 209.85.241.153 (209.85.241.153)  8.083 ms
 9  atl26s18-in-f14.1e100.net (172.217.164.78)  7.340 ms  8.828 ms  7.767 ms
pi@raspberrypi:~ $
```

Other Uses

- Besides communication and identification, what are some other reasons why these commands might be used?
  - could be used to diagnose issues on the network

Other Uses

- Having trouble communicating with another device?
  - use ping to verify if the device is active, experiencing issues, or completely down
- Experiencing issues on a certain website?
  - use traceroute to find the point in the path where the problem originates

- Through these commands, you can better understand the layout of your network and the devices on the network
  - **this can make recognizing and solving network issues much easier**

Resources

- https://www.man7.org/linux/man-pages/man8/ifconfig.8.html
- https://www.geeksforgeeks.org/iwconfig-command-in-linux-with-examples/
- https://www.howtogeek.com/355664/how-to-use-ping-to-test-your-network/
- https://linux.die.net/man/8/ping
- https://linux.die.net/man/8/traceroute

LAB

- complete the questions for Lab - Exploring the Network: Find Your Classmates