

Lab – Troubleshooting Using Network Utilities

Objectives

- Interpret the output of commonly used network command line utilities.
- Determine which network utility can provide the necessary information to perform troubleshooting activities in a bottom-up troubleshooting strategy.

Background/Scenario

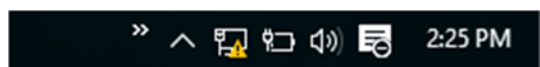
There are a number of problems that can cause networking connectivity issues. In this lab, you will use network utilities that can help you to identify connectivity issues in wireless networks. The network command line utilities are also useful to detect problems in a wired network.

Required Resources

- A computer with Windows 10 installed
- A wireless NIC installed
- An Ethernet NIC installed
- A Wireless Router
- Internet connectivity

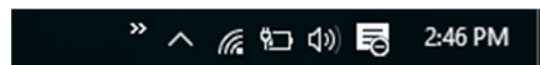
Step 1: Connect to a wireless network.

- Disconnect the Ethernet cable from your computer. An “orange triangle” appears over the Connections icon.

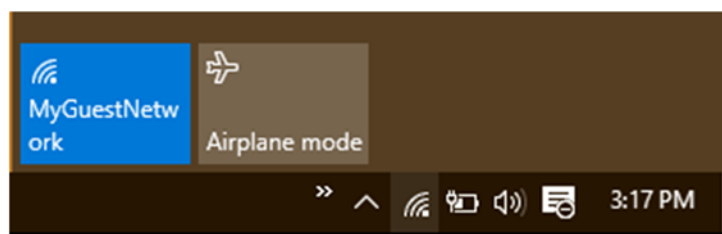


- Click the “Connections” icon in the tray. What is the name of an available wireless connection?

- Click one of the available wireless connections. Connect to the network. Enter login information if required. Confirm that the connection is successful.



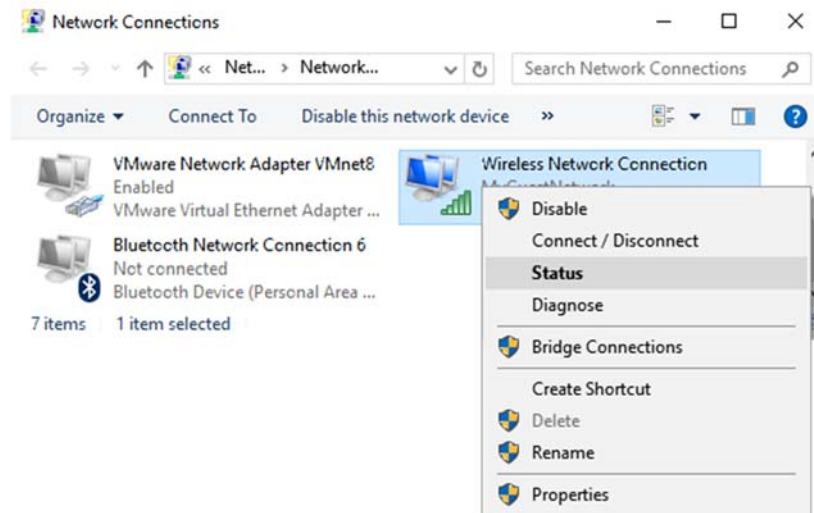
- Confirm that the connection is successful.



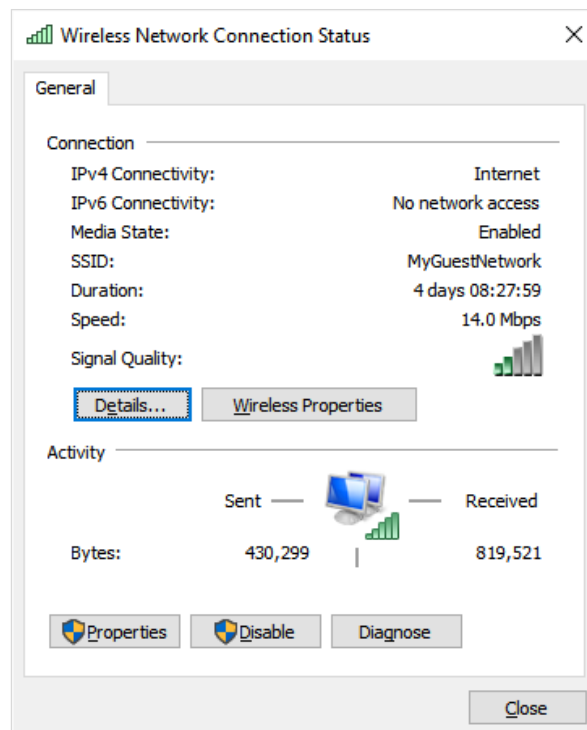
Step 2: Verify that the Network Adapter is operational.

When a connectivity problem is reported, the first step in a bottom-up troubleshooting strategy is to determine whether the NIC and the operating system settings on the computer are functioning correctly.

- Open the Control Panel, select **Network and Sharing Center**. Right-click **Start** and select **Control Panel**. Click **Network and Sharing Center**. Click **Change adapter settings**.
- Select the Wireless Network Connection. Right click on the adapter and select **Status** from the menu. If the **Status** choice is grayed out, it indicates that the adapter is either not enabled or not connected to a wireless SSID.



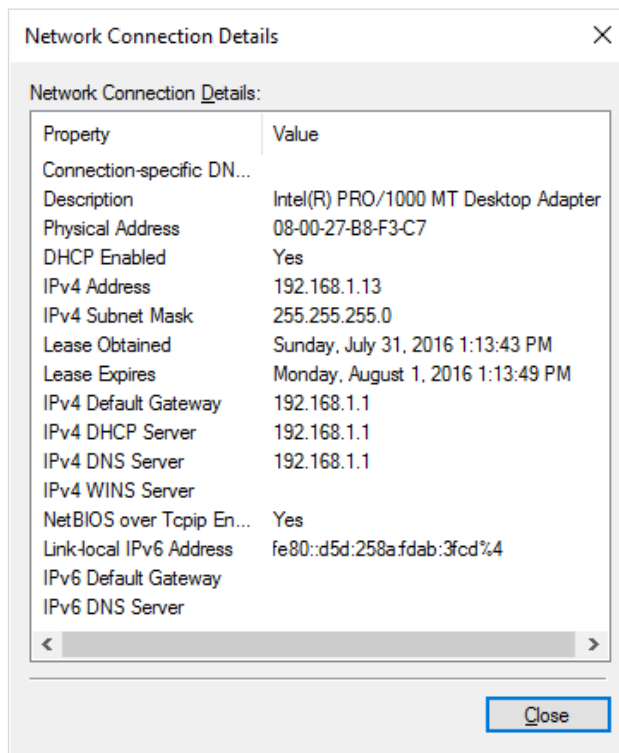
- When the status window opens, verify that the connection is enabled and that the connection SSID is correct. Click on **Details** to open the adapter details window.



- d. The Details window shows the current IP configuration active on the network adapter. It displays both the IPv4 and IPv6 configurations. If DHCP is active, the lease information is shown.

Is DHCP enabled on the PC? _____

When does the DHCP lease expire? _____



Step 3: Confirm the IP address configuration.

- a. Open a command window. Right-click **Start** menu and select **Command Prompt**.
- b. Enter **ping 127.0.0.1**. The IP address 127.0.0.1 is also referred to as the “localhost” address. A successful ping to the localhost address indicates that the TCP/IP protocol stack is operational on the computer. If the localhost address does not reply to a ping command, there might be an issue with the device driver or the network interface card.

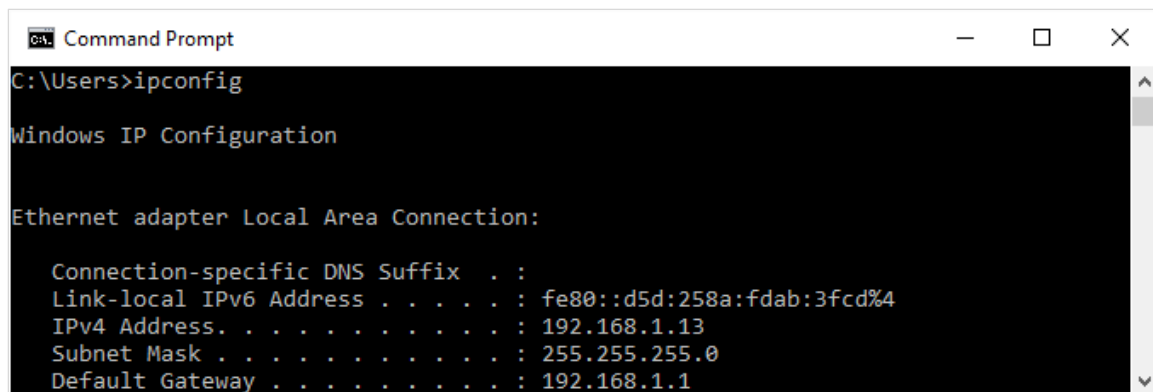
```
Command Prompt
C:\Users>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Was the **ping** command successful? _____

- c. Use the **ipconfig** command. Identify the IP address, subnet mask and default gateway addresses configured on the computer.



```
Command Prompt
C:\Users>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d5d:258a:fdab:3fcd%4
    IPv4 Address. . . . . : 192.168.1.13
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

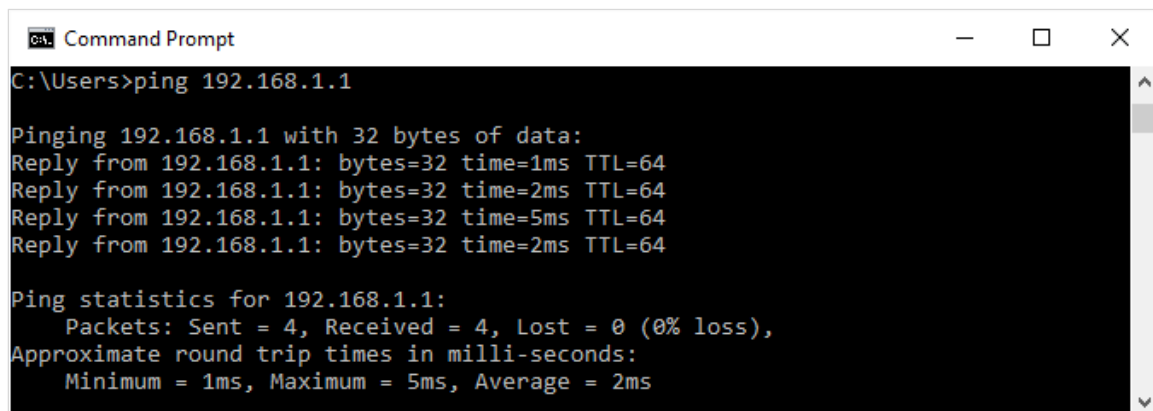
If the local IPv4 address is a host address on the 169.254.0.0/16 network, the computer received its IP address configuration through the Automatic Private IP Addressing (APIPA) feature of the Windows operating system.

What problems can cause a computer to receive an APIPA address?

If the computer is assigned an APIPA address, there might be an issue with the DHCP server. If the wireless router is providing the DHCP services, confirm that the DHCP service is configured correctly and that the IP address range is large enough to accommodate all of the devices that may attach wirelessly.

What is the IP address of the default gateway assigned to your PC? _____

To test whether or not the PC can reach the default gateway through the network, **ping** the default gateway IP address.



```
Command Prompt
C:\Users>ping 192.168.1.1

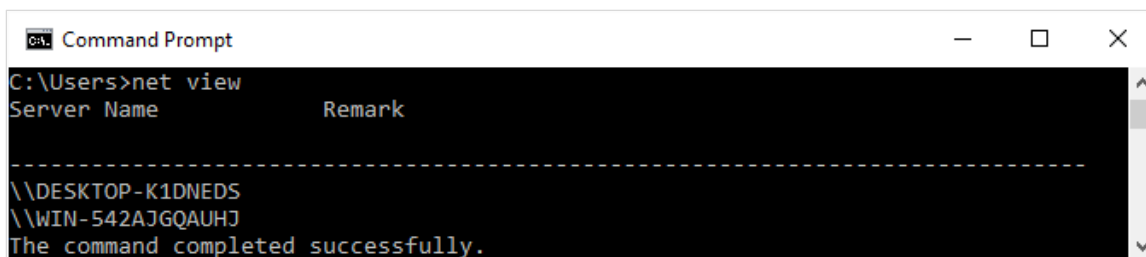
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

A successful ping indicates that there is a connection between the computer and the default gateway.

If the **ping** command does not complete successfully, make sure that the IP address of the gateway is typed correctly and that the wireless connection is active.

- d. Type **net view**. The **net view** command, when issued on a Windows PC, displays the computer names of other Windows devices in your Windows domain or workgroup. When **net view** displays the names of other computers it indicates that your computer is able to successfully send messages across the network.



```
C:\Users>net view
Server Name          Remark
-----
\\DESKTOP-K1DNEDS
\\WIN-542AJGQAUHJ
The command completed successfully.
```

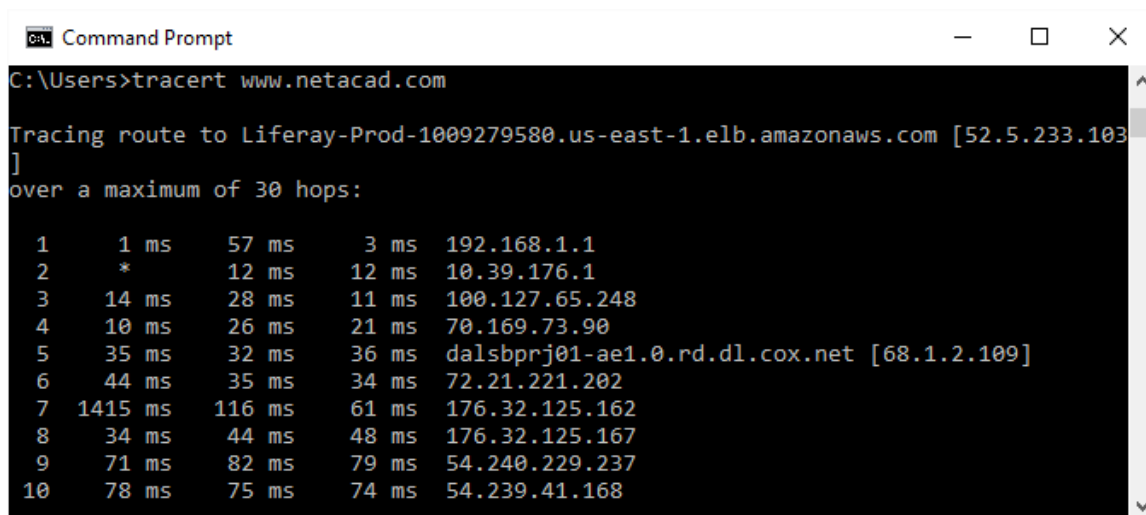
List the computer names that are displayed.

Note: Depending on the configuration of the PCs in your lab, **net view** may not return any computer names or may display an error message. If this is the case, move on to the next step.

Step 4: Test external connectivity.

If you have an external connection, use the following methods to verify the operation of the default gateway and the DNS service.

- a. The Windows **tracert** command performs the same function as the **traceroute** command used within the Cisco IOS. Use the **tracert** command along with your school's Web site URL or the Cisco Networking Academy Web site. Example: type **tracert www.netacad.com**. **Note:** Some output was omitted.



```
C:\Users>tracert www.netacad.com

Tracing route to Liferay-Prod-1009279580.us-east-1.elb.amazonaws.com [52.5.233.103]
over a maximum of 30 hops:

  1    1 ms    57 ms    3 ms    192.168.1.1
  2     *     12 ms    12 ms    10.39.176.1
  3    14 ms    28 ms    11 ms    100.127.65.248
  4    10 ms    26 ms    21 ms    70.169.73.90
  5    35 ms    32 ms    36 ms    dalsbprj01-ae1.0.rd.dl.cox.net [68.1.2.109]
  6    44 ms    35 ms    34 ms    72.21.221.202
  7   1415 ms   116 ms    61 ms    176.32.125.162
  8    34 ms    44 ms    48 ms    176.32.125.167
  9    71 ms    82 ms    79 ms    54.240.229.237
 10    78 ms    75 ms    74 ms    54.239.41.168
```

The **tracert** command displays the path that the packet takes between the source and destination IP addresses. Each router that the packet travels through to reach the destination address is shown as a hop in the **tracert** output. If there is a network issue on the path, the **tracert** output will stop after the last successful hop. The first hop in the output is the default gateway of the source PC, the last entry will be the destination address when the **tracert** command completes successfully.

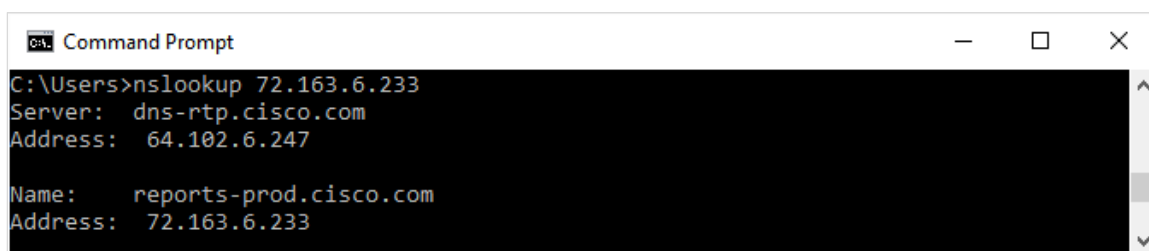
- b. **Tracert** uses the configured DNS server to resolve the fully qualified domain name to an IP address before beginning to trace the router to the destination. Using **tracert** or **ping** with a domain name instead of an IP address can confirm that the DNS server is providing name resolution services.

What IP address was returned by the DNS server? _____

What would happen if the DNS server could not resolve the domain name of the server?

- c. Use the **nslookup** command with the IP address you just discovered. **Nslookup** is a utility that can be used to troubleshoot DNS problems.

Type **nslookup 72.163.6.233**. The IP address in this example is assigned to a server at Cisco Systems. What domain name was returned?

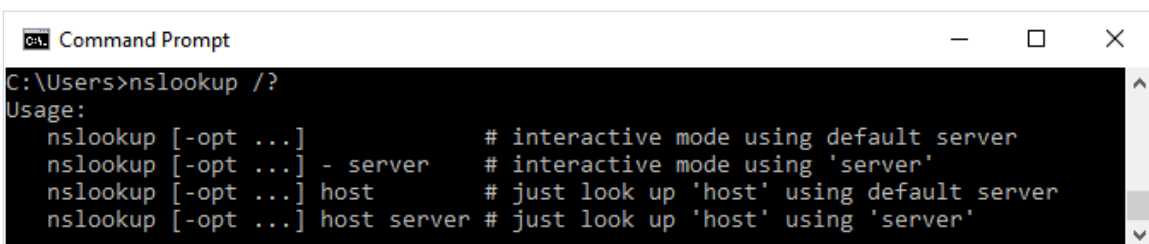


```
C:\Users>nslookup 72.163.6.233
Server:  dns-rtp.cisco.com
Address:  64.102.6.247

Name:    reports-prod.cisco.com
Address:  72.163.6.233
```

What DNS server did the **nslookup** command use to resolve the domain name?

Does the DNS server IP address match the one displayed in the **ipconfig /all** output? _____
When the configured DNS server cannot resolve domain names or IP addresses, it is possible to set **nslookup** to try to resolve the names using a different DNS server. If another DNS server can resolve the addresses, but the configured DNS server cannot, there could be a problem with the DNS server configuration. Type **nslookup /?** in order to view the options that can be used to test and troubleshoot DNS issues.



```
C:\Users>nslookup /?
Usage:
  nslookup [-opt ...]           # interactive mode using default server
  nslookup [-opt ...] - server  # interactive mode using 'server'
  nslookup [-opt ...] host      # just look up 'host' using default server
  nslookup [-opt ...] host server # just look up 'host' using 'server'
```

Step 5: Test Application layer connectivity.

- a. Open a web browser. Type **www.cisco.com** in the “Address” field, and then press **Enter**.



Does the Cisco.com web page load in the browser? What underlying network functions have to be working in order for the web page load?

Reflection

1. The steps in this lab represent a bottom-up troubleshooting strategy, where the effort starts with the OSI model Physical layer and finishes with verifying the functionality of the Application layer. What are the other two troubleshooting strategies used by network technicians to isolate problems?

2. Which strategy would try first when presented with a network connectivity problem? Why?
