Module 20: Troubleshoot Common Network Problems

Networking Essentials (NETESS)

Module Objectives

Module Title: Troubleshoot Common Network Problems
Module Objective: Troubleshoot basic network connectivity issues.

Topic Title	Topic Objective
The Troubleshooting Process	Describe some of the approaches used to troubleshoot networks.
Physical Layer Problems	Describe the process of detecting physical layer problems.
Troubleshooting Commands	Troubleshoot using network utilities.
Troubleshoot Wireless Issues	Troubleshoot a wireless network problem.
Common Internet Connectivity Issues	Explain common internet connectivity problems.
Customer Support	Explain how to use outside sources and internet resources for troubleshooting.

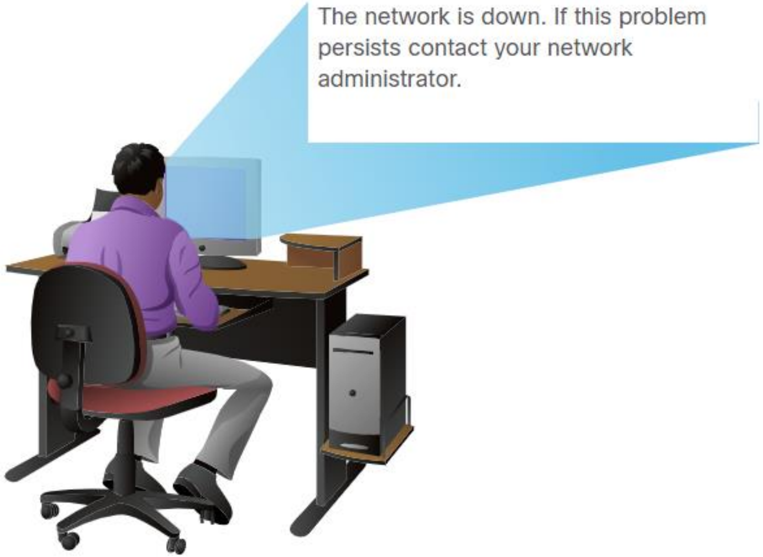
20.1 The Troubleshooting Process

The Troubleshooting Process

Network Troubleshooting Overview

Troubleshooting is the process of identifying, locating, and correcting problems. Documentation is part of the troubleshooting process and should include the following:

- A detailed description of the problem
- Steps taken to determine the cause of the problem
- Steps used to correct the problem


The network is down. If this problem persists contact your network administrator.

Gather Information

When gathering information, talk to the user and try to determine how much of the network is affected by the issue. Some things you might check for include the following:

Nature of problem

- End-user reports
- Problem verification report

Equipment

- Manufacturer
- Make / model
- Firmware version
- Operating system version
- Ownership / warranty information

Configuration and Topology

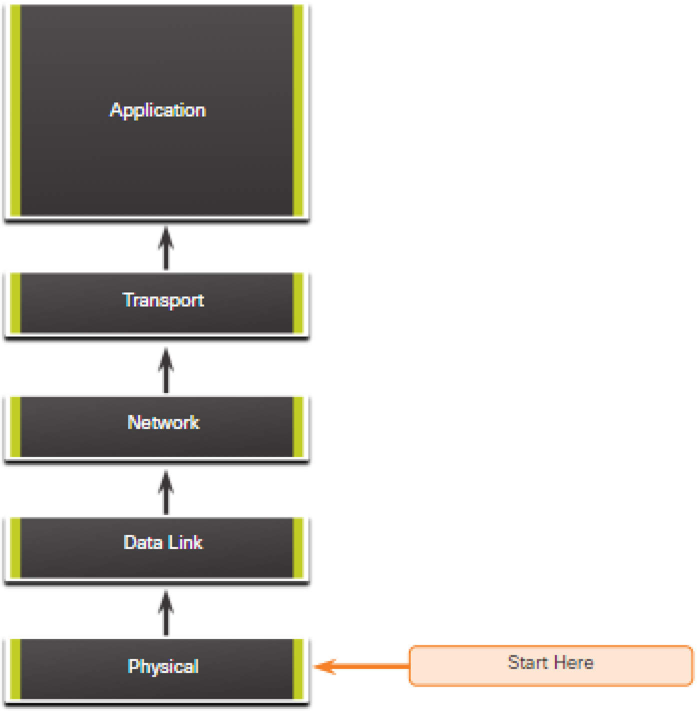
- Physical and logical topology
- Configuration files
- Log files

Previous Troubleshooting

- Steps taken
- Results achieved

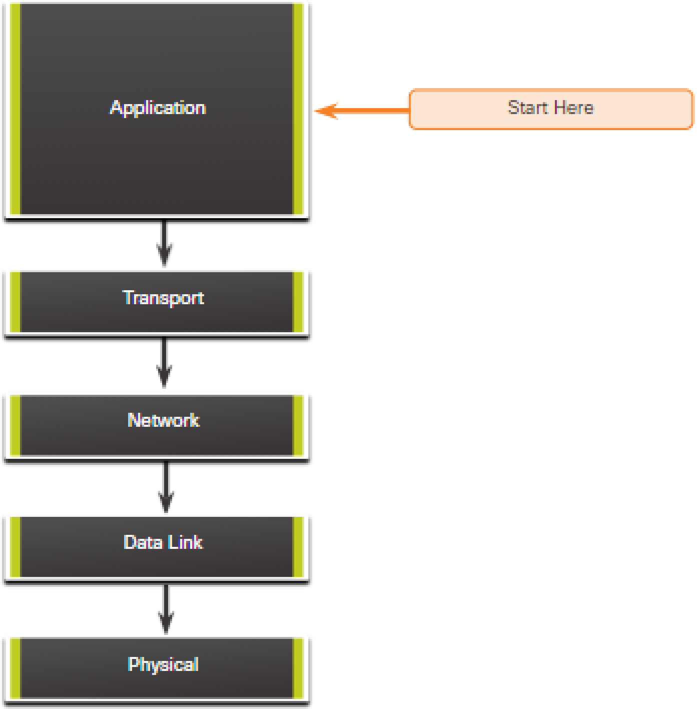
Structured Troubleshooting Methods – Bottom-Up

- Start with the physical layer and the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified.
- A good approach to use when the problem is suspected to be a physical one.
- Most networking problems reside at the lower levels, so implementing the bottom-up approach is often effective.
- A disadvantage is it requires that you check every device and interface on the network until the possible cause of the problem is found. It is also difficult to determine which devices to start examining first.



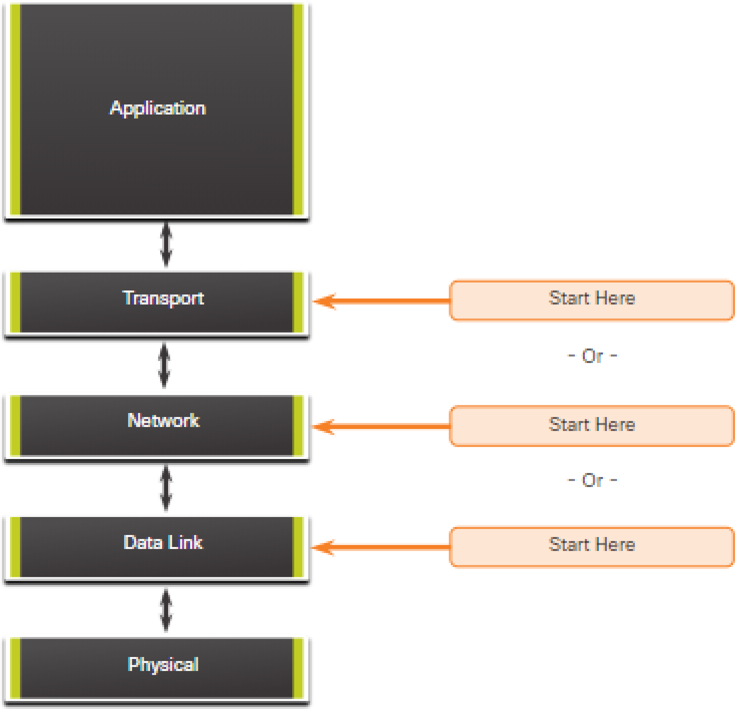
Structured Troubleshooting Methods (Cont.) – Top-Down

- Start with the end-user applications and move down through the OSI layers.
- End-user applications of an end system are tested before tackling the more specific networking pieces.
- Use this approach for simpler problems or when you think the problem is with a piece of software. The challenge is to determine which application to start examining first.
- Disadvantage is it requires checking every network application until the possible cause of the problem is found.



Structured Troubleshooting Methods (Cont.) – Divide-and-Conquer

- Select a layer and test in both directions.
- Start by collecting user experiences of the problem, document the symptoms and then, using that information, make an informed guess as to which OSI layer to start your investigation.
- When a layer is verified to be functioning properly, it can be assumed that the layers below it are functioning.
- Work up the OSI layers. If an OSI layer is not functioning properly, the administrator can work down the OSI layer model. For example, if users cannot access the web server, but they can ping the server, then the problem is above Layer 3. If pinging the server is unsuccessful, then the problem is likely at a lower OSI layer.



The Troubleshooting Process

Structured Troubleshooting Methods (Cont.) – Follow-the-Path and Substitution

Follow-the-Path

- One of the most basic troubleshooting techniques.
- First discover the traffic path all the way from source to destination.
- The scope of troubleshooting is reduced to just the links and devices that are in the forwarding path.
- The objective is to eliminate the links and devices that are irrelevant to the troubleshooting task at hand.
- This approach usually complements one of the other approaches.

Substitution

- Also called swap-the-component because you physically swap the problematic device with a known, working one. If the problem is fixed, then the problem is with the removed device. If the problem remains, then the cause may be elsewhere.
- Can be an ideal method for quick problem resolution, such as with a critical single point of failure. For example, a border router goes down. It may be more beneficial to simply replace the device and restore service, rather than to troubleshoot the issue.
- If the problem lies within multiple devices, it may not be possible to correctly isolate the problem.

Structured Troubleshooting Methods (Cont.) – Follow-the-Path and Substitution

Comparison

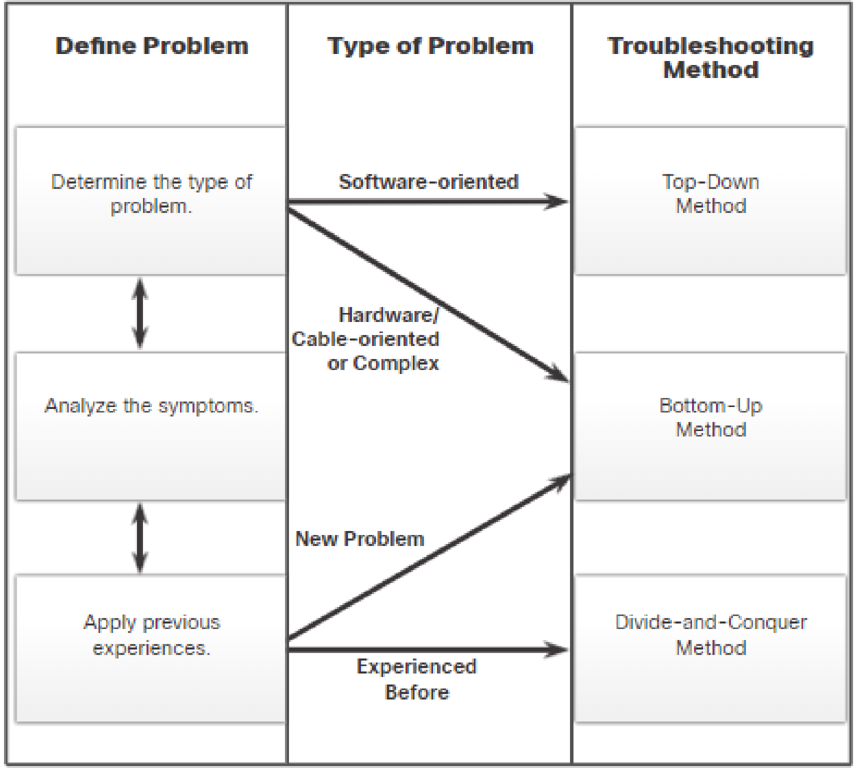
- Also called the spot-the-differences approach and attempts to resolve the problem by changing the nonoperational elements to be consistent with the working ones
- You compare configurations, software versions, hardware, or other device properties, links, or processes between working and nonworking situations and spot significant differences between them.
- The weakness of this method is that it might lead to a working solution, without clearly revealing the root cause of the problem.

Educated Guess

- Also called the shoot-from-the-hip troubleshooting approach
- A less-structured troubleshooting method that uses an educated guess based on the symptoms of the problem.
- Success of this method varies based on your troubleshooting experience and ability.
- Seasoned technicians are more successful because they can rely on their extensive knowledge and experience to decisively isolate and solve network issues.
- With a less-experienced network administrator, this troubleshooting method may too random to be effective.

Guidelines for Selecting a Troubleshooting Method

- Take the time to select the most effective network troubleshooting method.
- Software problems are often solved using a top-down approach.
- Hardware-based problems are solved using the bottom-up approach.
- New problems may be solved by an experienced technician using the divide-and-conquer method. Otherwise, the bottom-up approach may be used.



20.2 Physical Layer Problems

Common Layer 1 Problems

- A large proportion of networking problems are related to physical components or problems with the physical layer.
- Physical problems are concerned mainly with the hardware aspects of computers and networking devices, and the cables that interconnect them.
- Physical problems do not include the logical (software) configuration of devices.

Some of the more common Layer 1 problems include the following:

- Device receiving power? (turned off or unplugged)
- Loose network cable connection
- Incorrect cable type
- Faulty network cable
- Faulty wireless access point

Ensure there are no errors showing on any LEDs that display the connectivity status. If on-site, visually inspect all network cabling and reconnect cables to ensure a proper connection. If using wireless, verify that the device is operational and settings are configured correctly.

Common Layer 1 Problems (Cont.)

The Sense of Sight

- Cables which are not connected
- Cables connected to the wrong port
- Loose cable connections
- Damaged cables and connectors
- Use of the wrong type of cable
- View condition and function of various network devices with LEDs.

The Senses of Smell and Taste

- Smell can detect components which are overheating.
- Burning insulation or components is very distinct.
- Taste is directly related to the sense of smell because both use the same receptors such as tasting the acridness of something burning.

The Sense of Touch

- Feel for overheated components as well as to detect mechanical problems with devices such as cooling fans.
- Devices create a small vibration in the component that can be detected using touch.

The Sense of Hearing

- Used to detect major problems such as electrical issues and the proper operation of cooling fans and disk drives.
- All devices have characteristic sounds and any change from the normal sounds usually indicate a problem of some sort.

Physical Layer Problems

Wireless Router LEDs

- Examine LEDs (link lights) that indicate the current state or activity of a piece of equipment or connection.
- The exact configuration and meaning of LEDs varies between manufacturers and devices.
- Typical LEDs include ones for power, system, WLAN, wired ports, and internet (labeled WAN in the figure), USB, and Quick Security Setup (QSS, also known as Wi-Fi Protected Setup [WPS] that is a security risk).
- A normal condition is for these LEDs to flash indicating that traffic is flowing through the port.
- A solid green light typically indicates that a device is plugged into the port, but no traffic is flowing.
- No light typically indicates one or more of the following:
  - Nothing is plugged into the port.
  - There is an issue with the wired or wireless connection.
  - A device or port has failed.
  - There is a cabling issue.
  - The wireless router is improperly configured, for example, a port was administratively shut down.
  - The wireless router has a hardware fault.
  - The device does not have power.

Physical Layer Problems

Cabling Problems

- Be sure to use the correct type of cable.
- Check UTP cables (straight-through or crossover). Using the wrong type of cable may prevent connectivity.
- Improper cable termination is one of the main problems encountered in networks. Terminate using the T568A or the T568B standard. Avoid untwisting too much of the wire pairs during termination. Crimp connectors on the cable jacket to provide strain relief.
- Check maximum cable run lengths.
- Verify that the correct port is being used between devices.
- Protect cables and connectors from physical damage. Support cables to prevent strain on connectors and run cable through areas that will not be in the way.

20.3 Troubleshooting Commands

Overview of Troubleshooting Commands

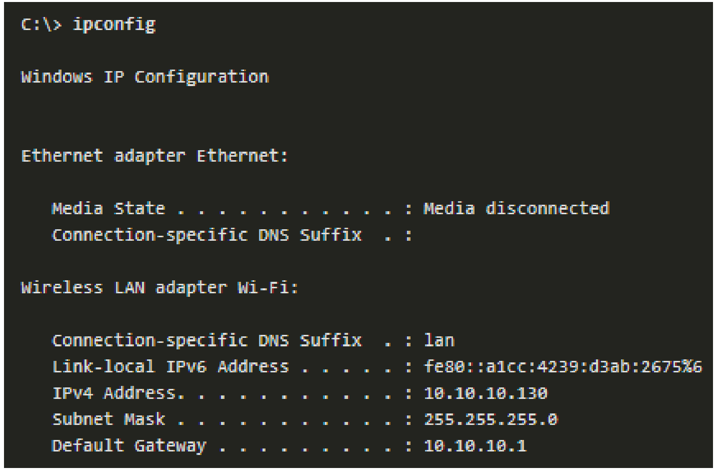
- Most of these utilities are provided by the operating system as command line interface (CLI) commands.
- The syntax for the commands may vary between operating systems.
- Some of the available utilities include:
  - **ipconfig** - Displays IP configuration information.
  - **ping** - Tests connections to other IP hosts.
  - **netstat** - Displays network connections.
  - **tracert** - Displays the route taken to the destination.
  - **nslookup** - Directly queries the name server for information on a destination domain.

Troubleshooting Commands

The ipconfig Command

ipconfig

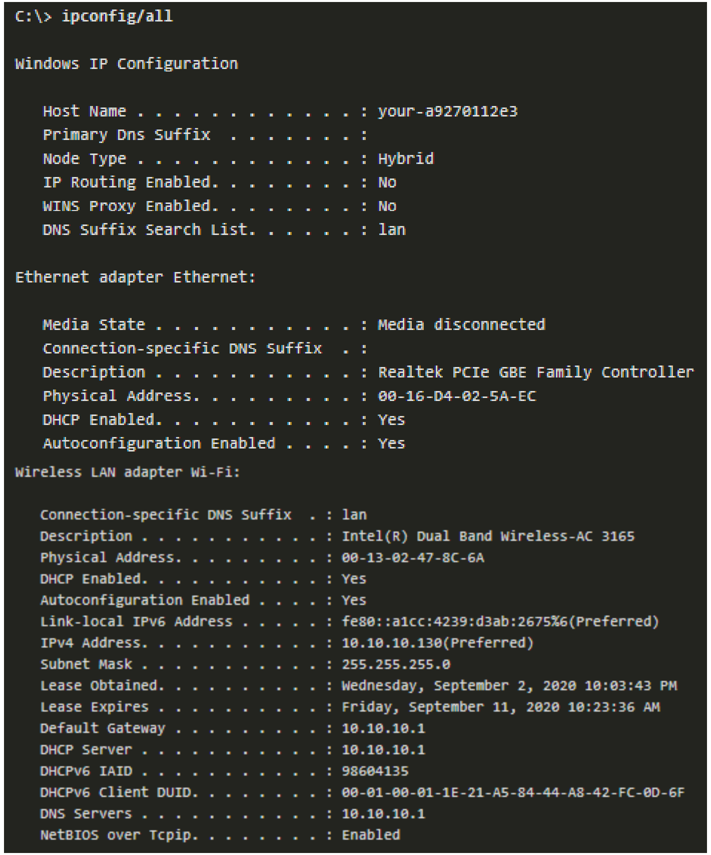
Used to display IP configuration information such as IP address, subnet mask, and default gateway



```
C:\> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   IPv4 Address. . . . . . . . . . . : 10.10.10.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

ipconfig /all

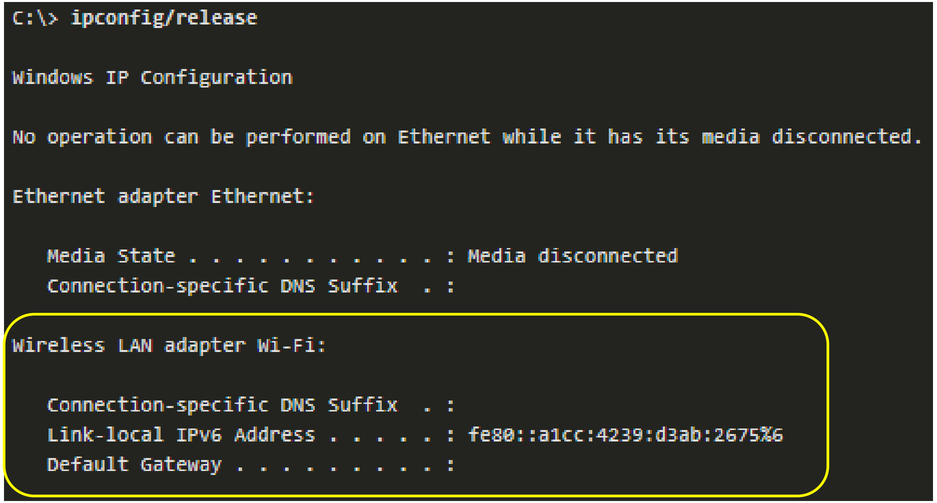
Includes MAC address, DNS server(s), and DHCP information



```
C:\> ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : your-a9270112e3
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : lan

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 00-16-D4-02-5A-EC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : 00-13-02-47-8C-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.130(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 2, 2020 10:03:43 PM
   Lease Expires . . . . . . . . . . : Friday, September 11, 2020 10:23:36 AM
   Default Gateway . . . . . . . . . : 10.10.10.1
   DHCP Server . . . . . . . . . . . : 10.10.10.1
   DHCPv6 IAID . . . . . . . . . . . : 98604135
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-21-A5-84-44-A8-42-FC-0D-6F
   DNS Servers . . . . . . . . . . . : 10.10.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

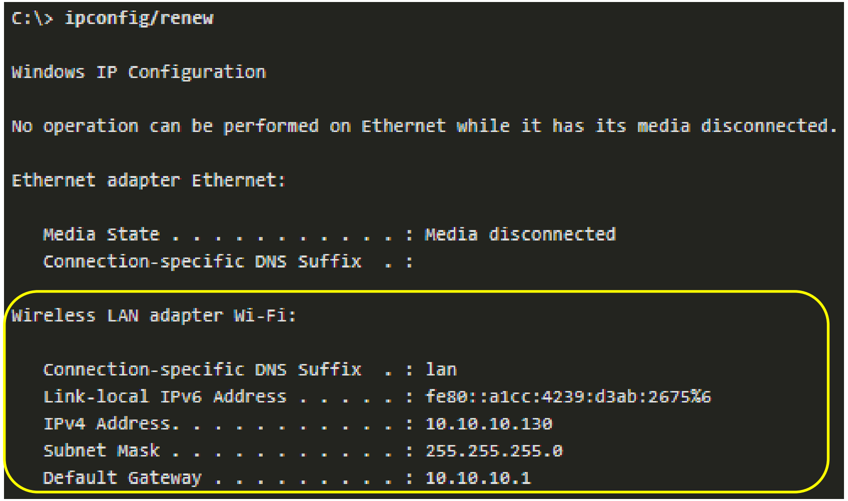
The ipconfig Command (Cont.) - /release and /renew

/release - used to let go of the current DHCP bindings



```
C:\> ipconfig/release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   Default Gateway . . . . . . . . . :
```

/renew - used to obtain new DHCP bindings



```
C:\> ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   IPv4 Address. . . . . . . . . . . : 10.10.10.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

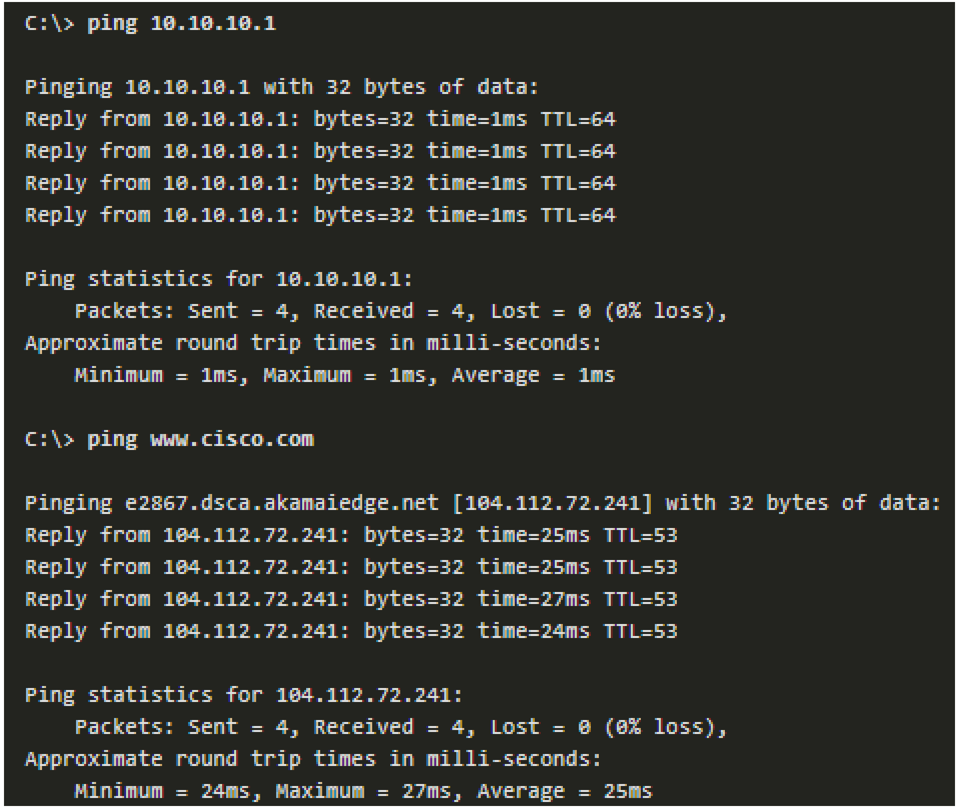
Troubleshooting Commands

Packet Tracer –Use the ipconfig Command

In this activity, you will use the **ipconfig** command to examine IP configuration information on a host.

The ping Command

- Most used network utility
- Tests whether or not network devices are reachable
- Echo request message used to send the packet
- Echo reply verifies connectivity
- Request timed out or general failure is an indication of failure
- A ping to a name like www.cisco.com verifies not only connectivity, but DNS as well.

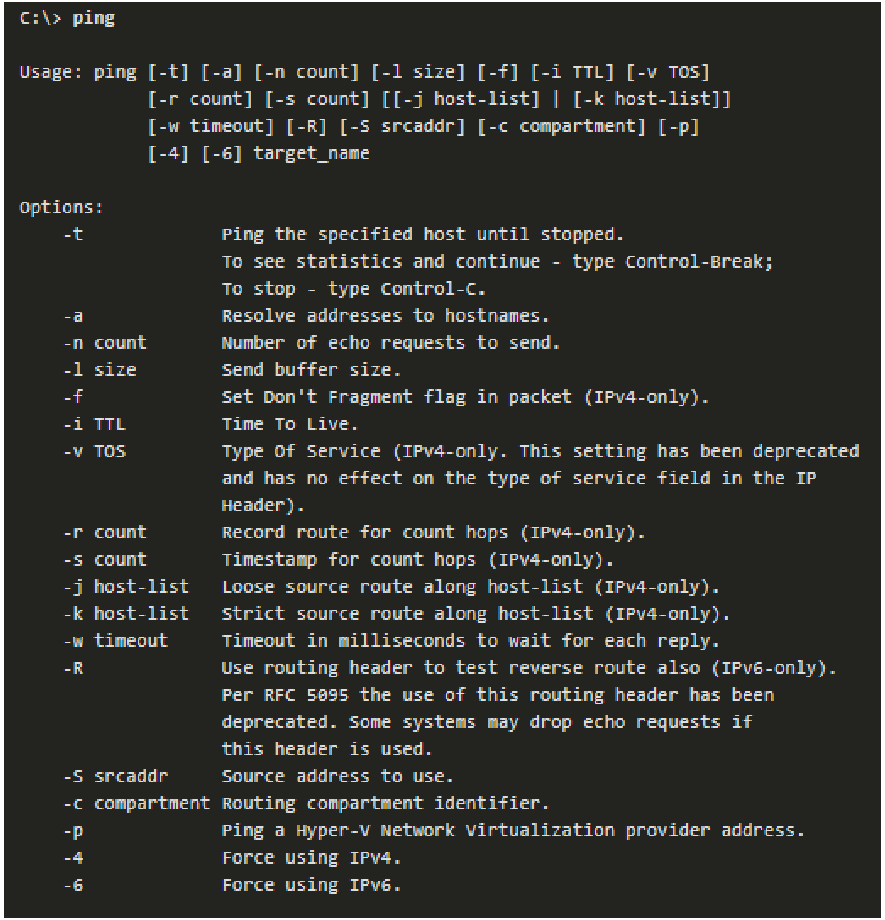


```
C:\> ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [104.112.72.241] with 32 bytes of data:
Reply from 104.112.72.241: bytes=32 time=25ms TTL=53
Reply from 104.112.72.241: bytes=32 time=25ms TTL=53
Reply from 104.112.72.241: bytes=32 time=27ms TTL=53
Reply from 104.112.72.241: bytes=32 time=24ms TTL=53

Ping statistics for 104.112.72.241:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 27ms, Average = 25ms
```

Troubleshooting Commands

Ping Results

- If neither a ping to an IP address, nor a ping to the name is successful, then network connectivity along the path to the destination is most likely the problem.
- Try to ping the default gateway.
- If the ping to the default gateway is successful, the problem is not local.
- If the ping to the default gateway fails, the problem resides on the local network.
- A ping may fail due to the firewall on the sending or receiving device, or a router along the path that is blocking the pings.

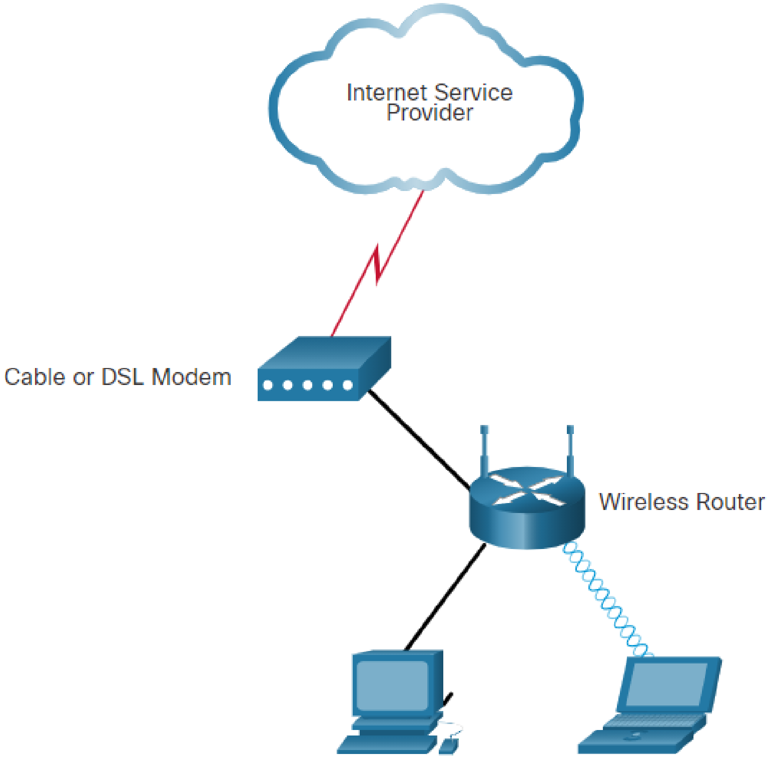


```
C:\> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Packet Tracer – Use the ping Command

In this activity, you will use the **ping** command to examine end-to-end connectivity between hosts.

Divide and Conquer with ping

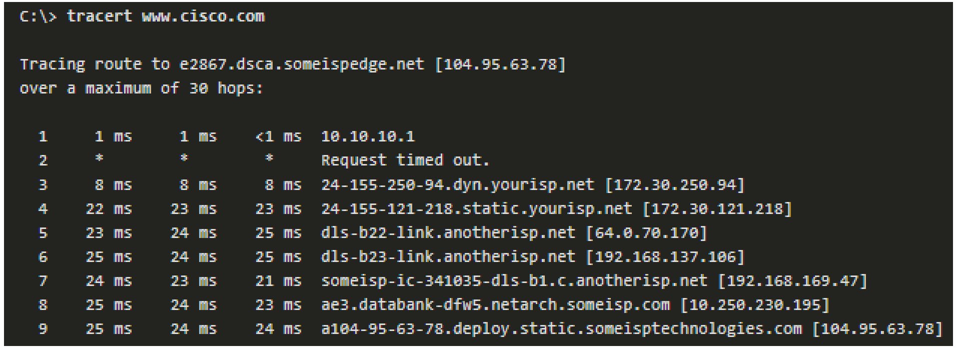


- Use a divide-and-conquer technique to isolate the problem to either the wired or the wireless network.
- Ping from a wired or wireless client to the default gateway. This verifies if the client is connecting as expected.
- Ping from the wireless client to a wired client. This verifies if the wireless router is functioning as expected.

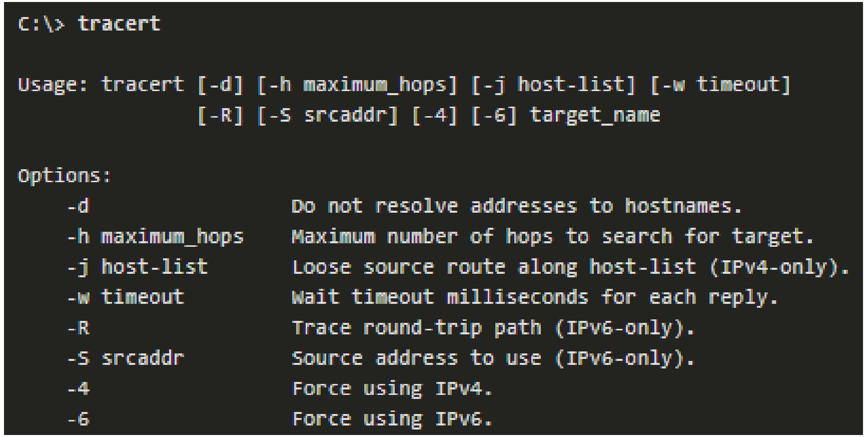
Troubleshooting Commands

The tracert Command

- The **ping** command does not indicate where a connection drops if it fails.
- Use **traceroute** (Microsoft and Linux) or **tracert** (Cisco and other OSes) to provide connectivity information about the path a packet takes to reach the destination and about every router (hop) along the way.
- Indicates how long a packet takes to get from the source to each hop and back (round trip time).
- Used to identify where a packet may have been lost or delayed due to bottlenecks or slowdowns.
- **Note**: Notice in the output that the 2nd hop failed. This is most likely due to a firewall configuration on that device which does not permit responding packets from the **tracert** command. However, the device does forward the packets to the next hop.



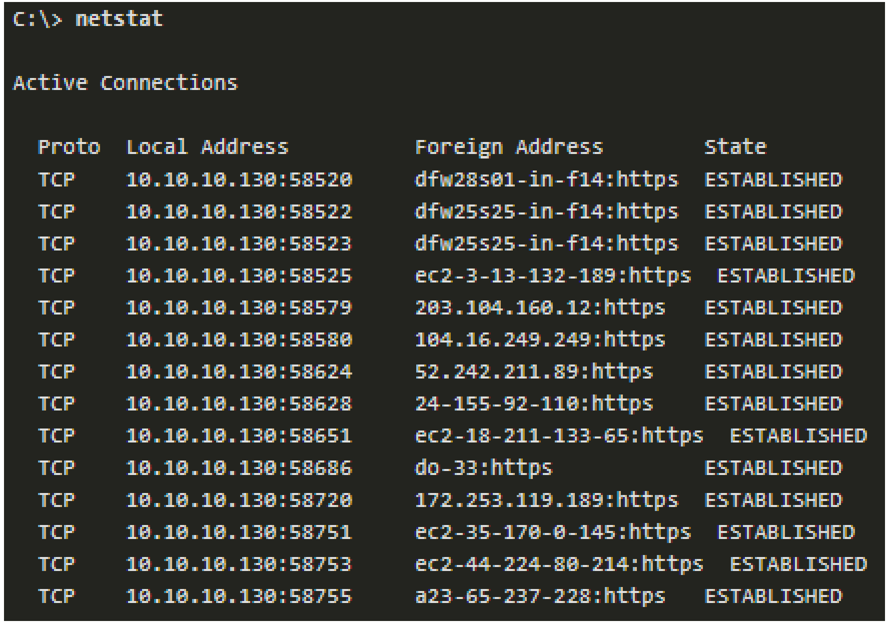
```
C:\> tracert www.cisco.com

Tracing route to e2867.dsca.someispedge.net [104.95.63.78]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  10.10.10.1
  2     *        *        *     Request timed out.
  3     8 ms     8 ms     8 ms  24-155-250-94.dyn.yourisp.net [172.30.250.94]
  4    22 ms    23 ms    23 ms  24-155-121-218.static.yourisp.net [172.30.121.218]
  5    23 ms    24 ms    25 ms  dls-b22-link.anotherisp.net [64.0.70.170]
  6    25 ms    24 ms    25 ms  dls-b23-link.anotherisp.net [192.168.137.106]
  7    24 ms    23 ms    21 ms  someisp-ic-341035-dls-b1.c.anotherisp.net [192.168.169.47]
  8    25 ms    24 ms    23 ms  ae3.databank-dfw5.netarch.someisp.com [10.250.230.195]
  9    25 ms    24 ms    24 ms  a104-95-63-78.deploy.static.someisptechnologies.com [104.95.63.78]
```



```
C:\> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

Troubleshooting Commands

The netstat Command



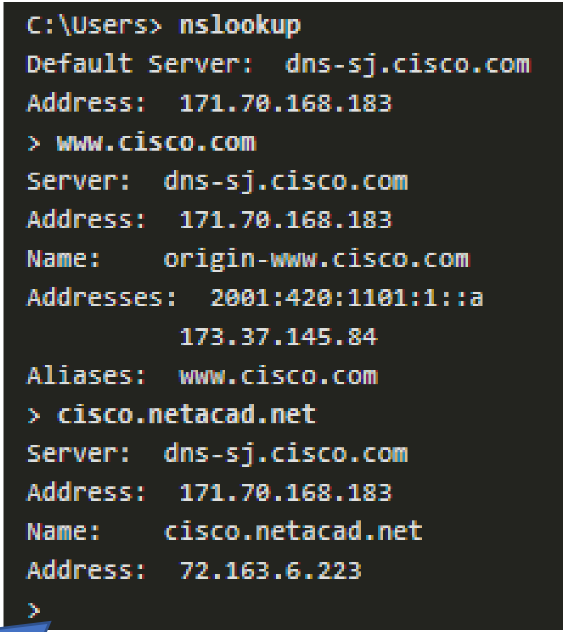
```
C:\> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.10.130:58520     dfw28s01-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58522     dfw25s25-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58523     dfw25s25-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58525     ec2-3-13-132-189:https  ESTABLISHED
  TCP    10.10.10.130:58579     203.104.160.12:https   ESTABLISHED
  TCP    10.10.10.130:58580     104.16.249.249:https   ESTABLISHED
  TCP    10.10.10.130:58624     52.242.211.89:https    ESTABLISHED
  TCP    10.10.10.130:58628     24-155-92-110:https    ESTABLISHED
  TCP    10.10.10.130:58651     ec2-18-211-133-65:https  ESTABLISHED
  TCP    10.10.10.130:58686     do-33:https            ESTABLISHED
  TCP    10.10.10.130:58720     172.253.119.189:https  ESTABLISHED
  TCP    10.10.10.130:58751     ec2-35-170-0-145:https  ESTABLISHED
  TCP    10.10.10.130:58753     ec2-44-224-80-214:https  ESTABLISHED
  TCP    10.10.10.130:58755     a23-65-237-228:https   ESTABLISHED
```

- The **netstat** command is used to verify active TCP connections and lists the protocol in use, the local address and port number, the foreign address and port number, and the state of the connection.
- Unexplained TCP connections can pose a major security threat because they can indicate that something or someone is connected to the local host.
- Unnecessary TCP connections can consume valuable system resources thus slowing down the host.

Troubleshooting Commands

The nslookup Command

- When a network device is being configured, one or more DNS server addresses are provided that the DNS client can use for name resolution.
- Usually the ISP provides the addresses to use for the DNS servers.
- When a user application requests to connect to a remote device by name, the requesting DNS client queries the name server to resolve the name to a numeric address.
- Nslookup allows the user to manually query the name servers to resolve a given host name.
- Can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- When issued, the default DNS server configured for your host is displayed. The name of a host or domain can be entered at the **nslookup** prompt.



```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```

Type exit to return to the prompt

Lab - Troubleshoot Using Network Utilities

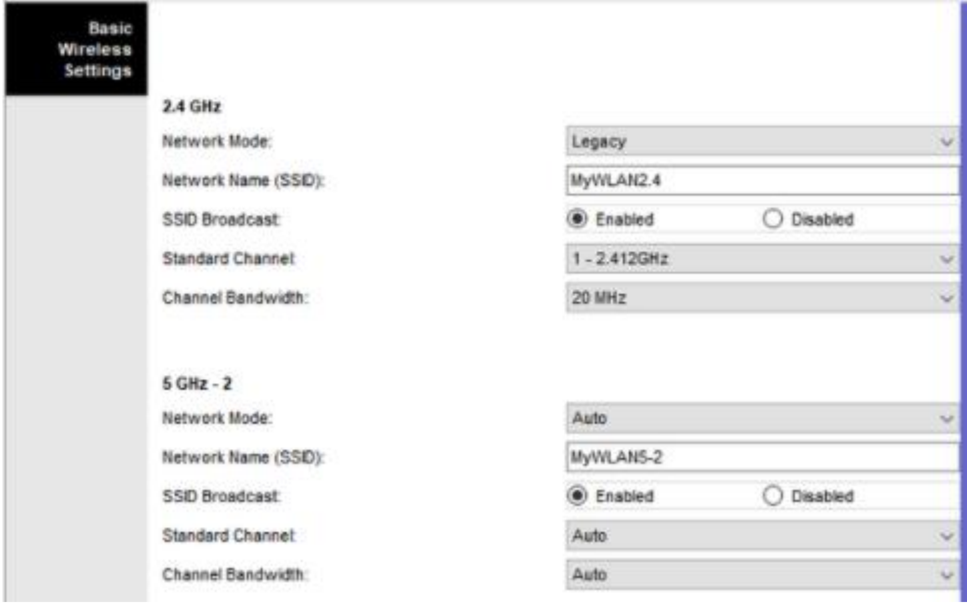
In this lab, you will complete the following objectives:

- 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.

20.4 Troubleshoot Wireless Issues

Troubleshoot Wireless Issues

Causes of Wireless Issues



Basic Wireless Settings

2.4 GHz

Network Mode: Legacy

Network Name (SSID): MyWLAN2.4

SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: 1 - 2.412GHz

Channel Bandwidth: 20 MHz

5 GHz - 2

Network Mode: Auto

Network Name (SSID): MyWLAN5-2

SSID Broadcast: ● Enabled ○ Disabled

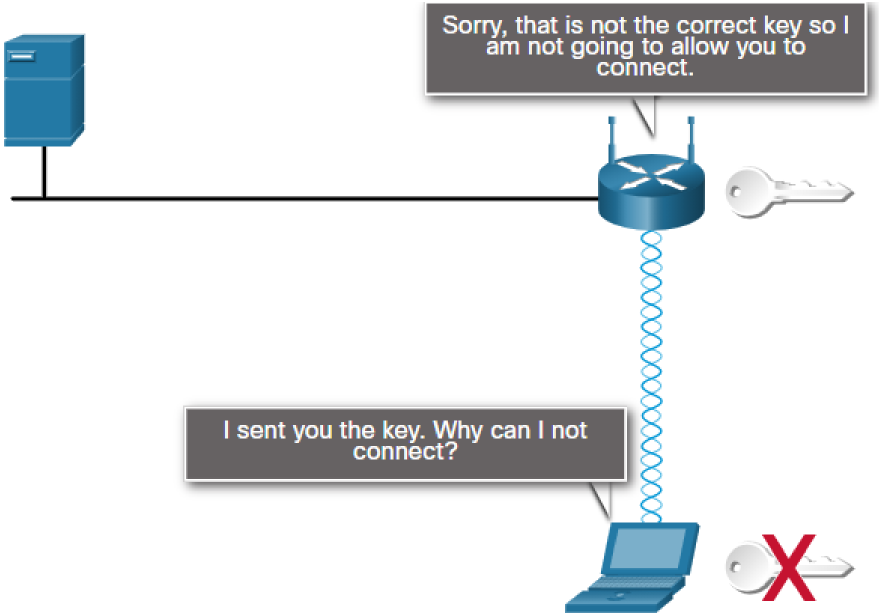
Standard Channel: Auto

Channel Bandwidth: Auto

- The 802.11ac (5 GHz band) is not compatible with the 802.11b/g/n standards (2.4 GHz band). Within the 2.4 GHz band, each standard uses different technology.
- Unless specifically configured, equipment that conforms to one standard may not function with equipment that conforms to another.
- In the figure, the 2.4 GHz network is configured to support legacy devices.
- Each wireless conversation must occur on a separate, non-overlapping channel that sometimes can be configured.
- The strength of an RF signal decreases with distance. Low signal strength causes devices to not connect or drop signals.
- Use the NIC client utility to display the signal strength and connection quality.
- RF signals are susceptible to interference from outside sources, including other devices functioning on the same frequency. Do a site survey to detect for this.
- APs share the available bandwidth between devices. As more devices associate with the AP, the bandwidth for each individual device will decrease causing network performance problems. The solution is to reduce the number of wireless clients using each channel.

Authentication and Association Errors

- The SSID is a case-sensitive, alphanumeric string that is up to 32-characters.
- The SSID must match on both the AP and client.
- If the SSID is not broadcast, it must be manually entered onto the client.
- If another AP is present that has broadcasted the SSID, the client may automatically associate to it.
- On most APs, open authentication is configured by default, allowing all devices to connect. If a more secure form of authentication is configured, a key is necessary.
- Both the client and the AP must be configured with the same key. If the keys do not match, authentication will fail, and the devices will not associate.
- If encryption is enabled, the same encryption key must be configured on both the AP and the client.


Sorry, that is not the correct key so I am not going to allow you to connect.
I sent you the key. Why can I not connect?

Troubleshoot Wireless Issues

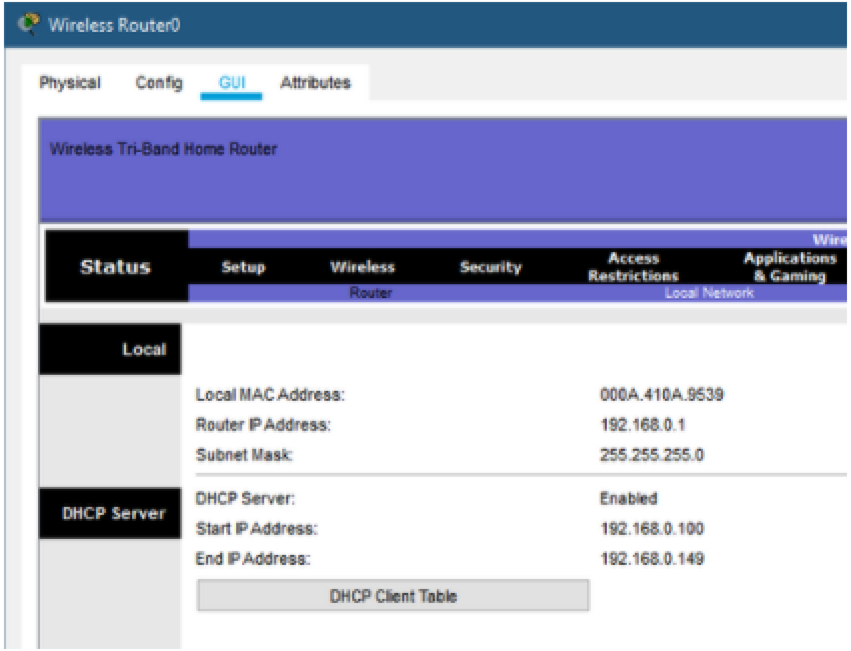
Packet Tracer – Troubleshoot a Wireless Connection

In this activity, you will be given a scenario. You will determine the reason why a wireless client is unable to connect to a wireless router and correct the problem.

20.5 Common Internet Connectivity Issues

DHCP Server Configuration Errors

- The IP configuration can have a major impact on the ability for a host to connect to the network.
- A wireless router can act as a DHCP server for local wired and wireless clients and provides IP configuration, including the IP address, subnet mask, default gateway, and commonly the IP addresses of DNS servers.
- The client table information should match the local host information, which you can see using the **ipconfig /all** command.
- If the client configuration information does not agree with information in the client table, the address should be released (**ipconfig /release**) and renewed (**ipconfig /renew**) to form a new binding.



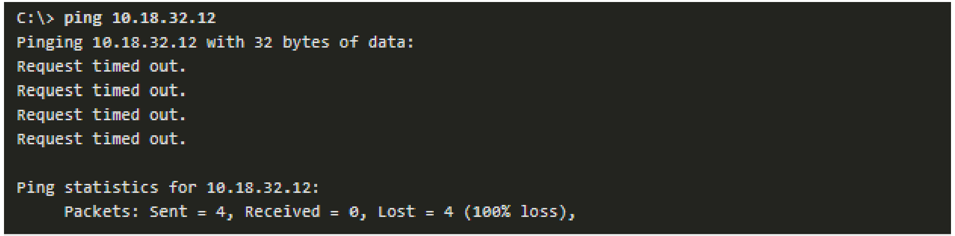
Local MAC Address: 000A.410A.9539
Router IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

DHCP Server: Enabled
Start IP Address: 192.168.0.100
End IP Address: 192.168.0.149

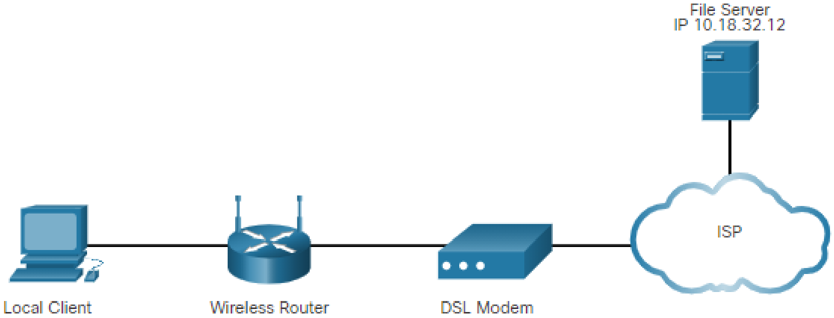
Common Internet Connectivity Issues

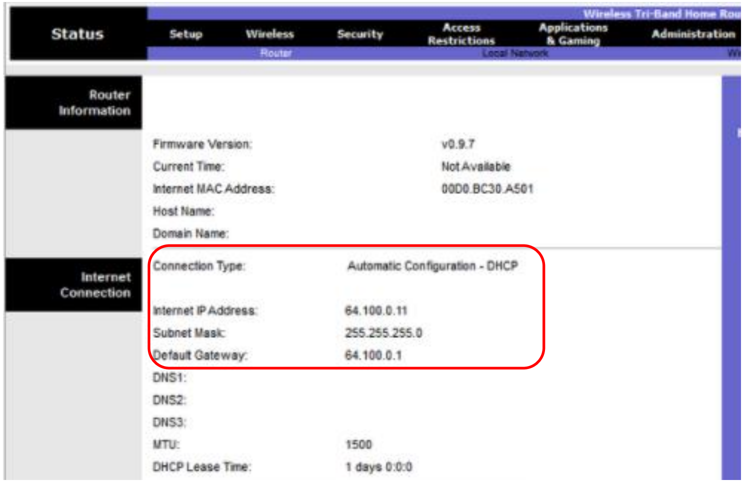
Check Internet Configuration

If hosts on the wired and wireless local network can connect to the wireless router and with other hosts on the local network, but not to the internet, the problem may be in the connection between the router and the ISP.



```
C:\> ping 10.18.32.12
Pinging 10.18.32.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.18.32.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```





Router Information

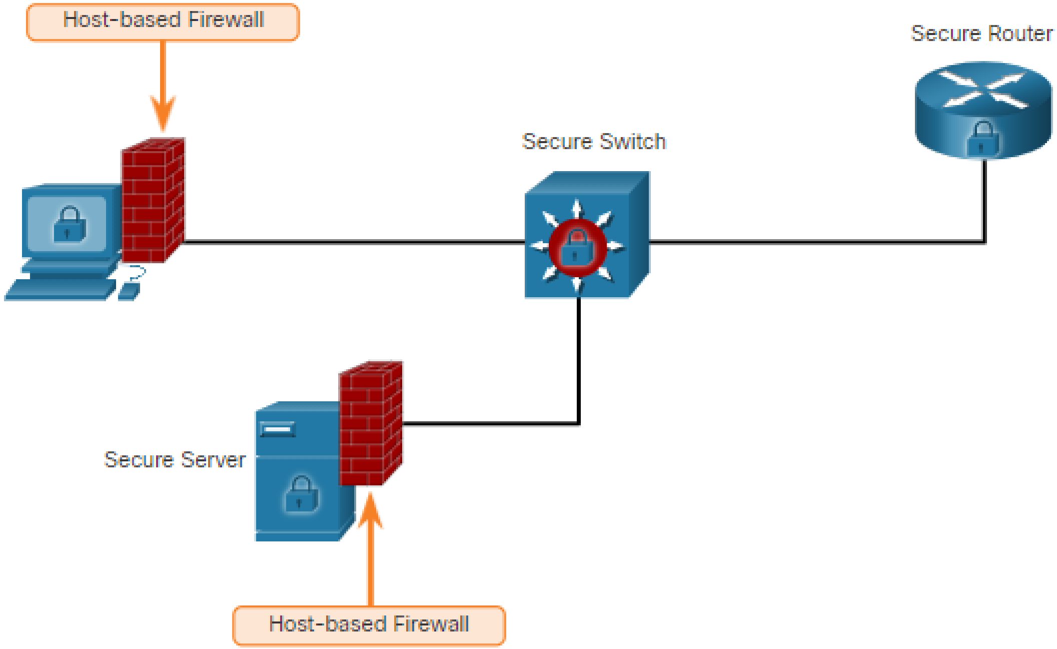
Firmware Version: v0.9.7
Current Time: Not Available
Internet MAC Address: 00D0.BC30.A501
Host Name:
Domain Name:

Internet Connection

Connection Type: Automatic Configuration - DHCP
Internet IP Address: 64.100.0.11
Subnet Mask: 255.255.255.0
Default Gateway: 64.100.0.1
DNS1:
DNS2:
DNS3:
MTU: 1500
DHCP Lease Time: 1 days 0:0:0

Check Firewall Settings

- If all clients are obtaining the correct IP configuration, and can connect to the wireless router but are unable to ping each other or cannot access a remote server or application, the problem may be with rules on the router.
- Check all settings on the router to ensure no security restrictions could be causing the issue.
- Verify that the local firewalls on the client devices are not preventing network functionality.



20.6 Customer Support

Sources of Help

- **Documentation** - Good documentation saves a great deal of time and effort by directing the troubleshooter to the most likely cause of the problem. It also provides the technical information required to isolate, verify, and correct the issue.
- **Online FAQs (Frequently Asked Questions)** - Most manufacturers provide a series of FAQs about their product or technology on their website. FAQs are a good source of current information and should be consulted whenever possible.
- **Internet searches** - Troubleshooters can now obtain assistance from people around the world in real time.
- **Colleagues** - Colleagues are often a wealth of information; there is no substitute for troubleshooting experience.

Customer Support

When to Call for Help

Support Desk: Good Afternoon Ms. Smith, Thank you for calling the support desk. My name is Pat. How may I be of assistance?

Customer: I cannot connect to the Cisco web site.

Support Desk: In order to help you I will have to gather some additional information.

- There are many ways to contact a support desk, including email, live chat, and phone.
- While email is good for non-urgent problems, phone or live chat is better for network emergencies.
- The support desk can take control of a local host through remote access software so support desk technicians to run diagnostic programs and interact with the host and network without having to physically travel to a job site.

Customer Support

Support Desk Interaction

- The support desk will require information on any service or support plans that are in place along with specific details of the affected equipment. This can include make, model, and serial number along with the version of firmware or operating system running on the device. They may also require the IP and MAC address of the malfunctioning device.
  - What symptoms were encountered?
  - Who encountered the problem?
  - When did the problem manifest?
  - What steps have been taken to identify the problem?
  - What were the results of steps taken?

Support Desk: When did this start to occur?

Customer: The Internet was working fine until 30 minutes ago.

Support Desk: Where do you live?

Customer: East of the river in Dodge City.

Support Desk: We are showing a lightning strike in that area. We have a team at the scene so connectivity should be restored within the hour.

Customer Support

Issue Resolution

- If the first-level support desk staff is unable to solve the problem they may escalate the problem to a higher level that are generally more knowledgeable and have access to resources and tools that the first-level support desk does not.
- Record all information regarding the interaction with the support desk.
  - Time/date of call
  - Name/ID of technician
  - Problem reported
  - Course of action taken
  - Resolution/escalation
  - Next steps (follow-up)

Customer Support

Support Desk Tickets and Work Orders

- The information gathering and recording process starts as soon as the technician answers the phone.
- After customer identification, the technician accesses the relevant customer information.
- Typically, a database application is used to manage the customer information.

20.7 Troubleshoot Common Network Problems Summary

Troubleshoot Common Network Problems Summary

Packet Tracer – Skills Integration Challenge

This activity includes many of the skills that you have acquired during your Networking Essentials studies. First, you will configure the IP addresses on network devices in a simplified network. Second, you will set up the wireless configurations in home network. Finally, you will verify your implementation by testing end-to-end connectivity by accessing the web server and router R1 using SSH in the simplified network.

What Did I Learn in this Module?

- Choose a troubleshooting approach to organize your efforts to fix the problem: top-down, divide-and-conquer, and bottom-up. Other good approaches are follow-the-path, substitution, comparison, and educated guess.
- To troubleshoot at Layer 1, check that all devices have power supplied and are on. Check LEDs.
- If the problem is with wireless, verify that the wireless access point is operational and that wireless settings are configured correctly.
- The **tracert** utility provides connectivity information about the path a packet takes to reach the destination and about every router (hop) along the way.
- **Netstat** can be used to verify active TCP connections.
- The **nslookup** utility allows an end user to look up information about a particular DNS name in the DNS server.
- Wireless issues can include compatibility with different standards, overlapping channels, RF signal strength from distance or interference, and too many devices sharing the bandwidth on a channel.
- Internet connectivity issues can include IP configuration issues from a DHCP server or the router getting configuration information from the ISP.
- A network firewall may prevent connectivity.
- Documentation is critical for network problem solving.

What Did I Learn in this Module? (Cont.)

- A problem may be escalated to a higher level where the staff are more knowledgeable and have access to additional resources and tools.
- Important information to be logged includes the time/date of call, name/ID of technician, problem reported, course of action taken, resolution/escalation, and next steps.
- Information for an incident is recorded and commonly in a knowledge base for future reference.

IPv4 and IPv6 Address Management Summary

New Terms and Commands

- troubleshooting
- documentation
- bottom-up method
- top-down method
- divide-and-conquer
- follow-the-path
- substitution
- comparison
- educated guess
- LEDs
- cable lengths
- **ipconfig**
- **ipconfig /all**
- **ipconfig /release**
- **ipconfig /renew**
- echo request
- echo reply
- shared bandwidth
- wireless interference
- firewall
- online Frequently Asked Questions (FAQs)
- Internet searches
- Colleagues
- remote access software
- trouble ticket
- incident report
- work order