CTS2134
Introduction to Networking

Module 10.4 – 10.7:
Troubleshooting

Interpreting ipconfig

Condition	ipconfig /all Output
Static IP	**DHCP Enabled = No and DHCP Server line will not be shown**
DHCP	**DHCP Enabled = Yes and DHCP Server = IP address of the DHCP server**
Alternate Configuration	**DHCP Enabled = Yes and DHCP Server line will not be shown** The IP address and subnet mask values will be a value other than the APIPA values. Default gateway and DNS server addresses will be configured using the alternate configuration values
APIPA	**DHCP Enabled = Yes and DHCP Server will not be shown** **IP address will be in the range of 169.254.0.1 to 169.254.255.254** **The Default Gateway line will be blank & DNS Servers will not be listed.** **The workstation sets its own IP address and mask.** Communication is restricted to APIPA hosts within the same subnet (no Default Gateway set). If some hosts are still using an address assigned by the DHCP server, these hosts will not be able to communicate with the APIPA hosts. Name resolution will not be performed (no DNS server set).

Interpreting ipconfig

Condition	ipconfig /all Output
Rogue DHCP Server	**A Rogue DHCP server is an Unauthorized DHCP server.** •**May have Conflicting IP addresses** on the network •**May have Incorrect IP configuration** information on some hosts •**Use ipconfig and verify the DHCP server address.** If this address is not the address of your DHCP server, you have a rogue DHCP server. •Some hosts may receive configuration information from the correct DHCP server and some from the rogue DHCP server.
Incorrectly Configured DHCP Server	If network hosts are configured with incorrect IP values, first verify that the workstations are contacting the correct DHCP server. If the correct server is being used, go to the DHCP server and verify that it is sending out the correct configuration information.
If the workstation has received configuration information from the wrong DHCP server or configured itself using APIPA, you need to retry to contact the DHCP server once DHCP problems have been resolved. Use the following commands: Use **ipconfig /release** to stop using the current dynamic IP configuration parameters. Use **ipconfig /renew** to retry the DHCP server request process	

arp, netstat, and nbtstat Facts

Tool	Option(s)
arp	**arp -a** shows the IP address-to-MAC address mapping table
netstat	**netstat** shows the active connections **netstat -a** shows detailed information for active connections **netstat -r or route print** shows the routing table of the local host **netstat -s** shows TCP/IP statistics
nbtstat	**nbtstat -c** shows the IP address-to-NetBIOS name mapping table
Local computers have a cache of recently-used IP addresses and their corresponding MAC addresses. The cache can cause problems if the MAC address for a computer has recently changed, such as if the network interface card has been replaced. To correct the problem, use the **netsh** command to clear the ARP cache.	

Troubleshooting Name Resolution

With Name Resolution problems, you can ping a destination host using its IP address but methods that use the logical host name to communicate with the host fails.

This might include things such as:

- Typing a URL into the browser.
- Pinging the host using the host name.
- Searching for the host by its name.

To troubleshoot DNS name resolution, use one of the following tools:

- **nslookup** for Windows
- **dig** or **host** for Linux systems

Local computers have a cache of recently-resolved DNS names. If the name is in the cache, the corresponding IP address will be used. If the IP address of a host has changed, this makes communication using DNS impossible. To correct this problem, run **ipconfig /flushdns** to delete the local DNS name cache.

Switch Troubleshooting Facts

Issue	Description
Collisions	*A collision occurs when two devices that share the same media segment transmit at the same time.* In a switched network, collisions should only occur on ports that have multiple devices attached. To eliminate collisions, connect only a single device to each switch port.
Broadcast Storms	*A broadcast storm is excessive broadcast traffic that renders normal network communications impossible.* To reduce broadcast storms: • Use VLANs to create separate broadcast domains on switches. • Run the spanning tree protocol to prevent switching loops. • Implement switches with built-in broadcast storm detection.
Switching Loop	*A switching loop occurs when there are multiple active paths between two switches.* Switching loops lead to incorrect entries in a MAC address table, making a device appear to be connected to the wrong port and causing unicast traffic being circulated in a loop between switches.

Switch Troubleshooting Facts

Issue	Description
Duplex mismatch	*A duplex mismatch occurs when two devices are using different duplex settings.* By default, devices are configured to use autonegotiation to detect the correct duplex setting to use. A duplex mismatch can occur in the following cases: • Both devices are configured to use different duplex settings. • Autonegotiation does not work correctly on one device. • One device is configured for autonegotiation and the other device is manually configured for full duplex.
Frame errors	*The switch examines incoming frames and will only forward frames that are complete and correctly formed, while invalid frames are simply dropped.* • Frames that are too long are typically caused by a faulty network card that jabbers (constantly sends garbage data). • Frames that are too short are typically caused by collisions. • CRC errors indicate that a frame has been corrupted in transit. • All types of frame errors can be caused by faulty cables or physical layer devices.

Switch Troubleshooting Facts

Issue	Description
Slow Link Speed	Most network components are capable of supporting multiple network specifications. If you find that the speed in use on a segment is lower than expected: • Check individual devices to verify that all support the higher speed. • Check individual devices to see if any have been incorrectly configured. • Use a cable certifier to verify that the cables meet the rated speeds.
Incorrect VLAN Member-ship	VLANs create logical groupings of computers based on switch port. Because devices on one VLAN cannot communicate with devices in different VLANs, incorrectly assigning a port to a VLAN might prevent a device from communicating through the switch. **Note: VLAN membership is defined by switch port, not by MAC address.** On the switch, verify that ports are assigned to the correct VLANs, and that any unused VLANs are removed from the switch.

Switch Troubleshooting Facts

Issue	Description
Duplex mismatch	*A duplex mismatch occurs when two devices are using different duplex settings.* By default, devices are configured to use autonegotiation to detect the correct duplex setting to use. A duplex mismatch can occur in the following cases: • Both devices are configured to use different duplex settings. • Autonegotiation does not work correctly on one device. • One device is configured for autonegotiation and the other device is manually configured for full duplex.
Frame errors	*The switch examines incoming frames and will only forward frames that are complete and correctly formed, while invalid frames are simply dropped.* • Frames that are too long are typically caused by a faulty network card that jabbers (constantly sends garbage data). • Frames that are too short are typically caused by collisions. • CRC errors indicate that a frame has been corrupted in transit. • All types of frame errors can be caused by faulty cables or physical layer devices.

Troubleshooting Routing Facts

Problem	Description
Can't access hosts outside the local subnet	If one or more hosts can only communicate with hosts on the local subnet, the problem is likely with the default gateway configuration. • If a single host is having problems, verify the default gateway setting on that host. • If multiple hosts are having problems, verify the default gateway setting, and verify that the DHCP server is configured to deliver the correct default gateway address. • If all hosts have the same problem, and if the default gateway setting is correct, verify that the default gateway server is up and configured for routing.

Troubleshooting Routing Facts

Problem	Description
Can't communicate with any host on a specific network	If hosts are unable to contact hosts on a specific subnet, but communication with other subnets is working, check the following: • Verify that the router connected to the subnet is up. • Use the **route command on the default gateway of the local subnet** and verify that the router has a route to the remote subnet. If necessary, configure a static route or a routing protocol so the route can be learned automatically. • Use **traceroute to view the route taken to the destination network.** • Check for ***routing loops in the path to the destination network***. A routing loop is caused by a misconfiguration in the routers. Routing loops are indicated by: • Routing table entries that appear and then disappear (called *route flapping),* often at regular intervals (such as every minute). • Routing table entries where the next hop router address oscillates (changes) between two or more different routers. • **Traceroute** output that displays the same sequence of routers being repeated.

Troubleshooting Routing Facts

Problem	Description
Can't access the Internet	If hosts are able to reach all internal networks but can't access the Internet, check for the following: • Verify that the Internet connection is up. • Check for a default route on the router connected to the Internet. A default route is indicated by a network address of 0.0.0.0 with a mask of 0.0.0.0. The default route is used for all packets that do not match another entry in the routing table. **Note:** Most routers connecting private networks to the Internet do not know about specific networks and routes on the Internet. In addition, most routers do not share routes for private subnets with Internet routers. Instead, the router is configured with a single default route that is used for all Internet traffic, and a router at the ISP is responsible for sharing a single route into your private network with other Internet routers.

Troubleshooting Routing Facts

Problem	Description
Remote clients can't access network	If you have remote access clients who can establish a connection to the remote access server, but can't connect to other resources on the private network, check the following: • If remote clients are being assigned an IP address on the same subnet as the private network, make sure that proxy ARP is enabled on the LAN interface of the remote access server. Proxy ARP is required to make it appear as if the remote clients are connected to the same network segment. • If remote clients are being assigned an IP address on a different subnet than the private network, make sure the remote access server has routing configured to route packets between the remote clients and the private network.