6.9.9 TCP/IP Utilities

The following table describes the various command utilities you can use to troubleshoot network issues:

Utility	Description
ipconfig (Windows OS)	**ipconfig** displays IP configuration information for network adapters. Use the **ipconfig** command as follows: ▪ Use **ipconfig** to view IP address, subnet mask, and default gateway configuration. ▪ Use **ipconfig /all** to view detailed configuration information, including the MAC address and the DHCP server used for configuration. ▪ Use **ipconfig /release** to release the IP configuration information obtained from the DHCP server. ▪ Use **ipconfig /renew** to request new IP configuration information from the DHCP server. ▪ Use **ipconfig /displaydns** and **ipconfig /flushdns** to view and manage the local DNS cache. The first command displays the contents of the local DNS cache that Windows maintains and updates every 24 hours. The second option flushes (or removes) all the entries in the current DNS cache. If the IP address of a network server is changed, your local cache will contain the old IP address until the cache is updated or the **flushdns** option is used.
ifconfig (Linux/macOS)	**ifconfig** is used on Linux and macOS systems and displays the installed network interfaces and the current configuration settings for each interface, including the MAC address, IP address, broadcast address, and subnet address. Use the **ifconfig** command as follows: ▪ Use **ifconfig -a** to display all the interfaces which are currently available, even if the interface is down. ▪ Use **ifconfig** *[interface_name]* **down** to disable the specified network interface. ▪ Use **ifconfig** *[interface_name]* **up** to enable the specified network interface. Use the following utilities to display additional networking information not provided by ifconfig: ▪ The **hostname** command displays the system's hostname. ▪ The **route** command displays the default gateway configuration settings. On Linux systems, the **iwconfig** command is used to display information about wireless network interfaces.

ip addr	Displays the current networking information.
	▪ **ip addr** or **ip addr show**
	Shows the addresses assigned to all the network interfaces.
	▪ Common **ip addr show** parameters include the following:
	  ▪ **inet** shows the IPv4 address with the subnet mask in CIDR notation.
	  ▪ **brd** shows the broadcast address.
	  ▪ **up** or **down** shows the interface status.
	  ▪ **inet6** shows the IPv6 IP address.
	  ▪ *interface name* show the networking information for the specified interface.
	  Example: **ip addr show enp2s1**

ping	**ping** sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them. You can ping a host by IP address or use the DNS name. When the DNS name is used, the computer must look up the corresponding IP address before performing the ping test. ▪ **-a** looks up the hostname from a given IP address. ▪ **-t** performs a continuous ping test (press **Ctrl** + **C** to stop sending the ping tests). ▪ **-l** ***[size]*** specifies the packet payload size (in bytes) to use in the test. This can help determine whether packets above a certain size are being lost.
tracert, **traceroute**	**tracert** is similar to the **ping** utility because it tests connectivity between devices; however, **tracert** also shows the path between the two devices. Responses from each hop on the route are measured three times to accurately report how long the packet takes to reach the specific host and then return. ▪ On a Windows system, use the **tracert** command. ▪ On Linux and macOS systems, use the **traceroute** command.
nslookup	**nslookup** resolves (looks up) the IP address of the specified hostname. It also displays additional name resolution information, such as the DNS server used for the lookup request.
netstat	**netstat** displays the following IP-related statistics: ▪ Current connections ▪ Incoming and outgoing connections ▪ Active sessions, ports, and sockets ▪ The local routing table
nbtstat	**nbtstat** is used to diagnose issues regarding NetBIOS over TCP/IP. You can use the following options with **nbtstat**: ▪ **-c** displays the NetBIOS cache of remote machine names and their IP addresses. ▪ **-n** displays NetBIOS names that have been registered on the local system. ▪ **-r** displays names resolved by broadcast and via WINS. ▪ **-R** clears and then reloads the remote cache name table. ▪ **-S** displays current NETBIOS sessions with the destination IP addresses. ▪ **-s** displays current NETBIOS sessions by NETBIOS names.
Telnet	The Telnet utility is used for remote server management. ▪ The Telnet protocol must be running and configured on the remote server in order for a Telnet session to be established. ▪ By default, Telnet does not encrypt transmissions (they are sent as clear text). ▪ Telnet is mostly used by specialized industrial and scientific devices. In addition to sending transmissions in clear text, there are several well-known vulnerabilities in the Telnet protocol. Because of this, Telnet should not be used when sending sensitive information.

SSH	Like Telnet, the SSH utility is used for remote server management; however, SSH encrypts all communications and is much more secure. ▪ SSH can be used to remotely log onto a server and complete configuration tasks. ▪ In order to establish an SSH session, the server must have the SSH process running and configured to allow remote connections. ▪ Use the following syntax to establishing an SSH connection: **ssh** *[username]@[server_address]*