# 11.2.2 Network Monitoring Facts

The goal of monitoring is to keep track of conditions on the network, identify situations that might signal potential problems, pinpoint the source of problems, and locate areas of your network that might need to be upgraded or modified.

As you monitor your network, look for the top talkers and listeners.

- Top talkers are computers that send the most data, either from your network or into your network.
- Top listeners are hosts that are receiving most of the data by streaming or downloading large amounts of data from the internet.

It is important to know which computers are the big receivers and senders of information because it is a good way to tell if something is wrong on your network. An unauthorized system that is sending large amounts of data to locations outside of your network could be a sign of a data breach.

The below table lists some of the tools used to monitor the health of a network:

| Tool | Description |
|---|---|
| ping | Ping is a command line tool that is used to perform a connection test between two network devices. Ping works by sending ICMP packets to a specified device on the network and waiting for a response. This shows if there is a connection issue or not. The syntax for the ping command is:<br>**ping <target IP address or hostname>**<br>The following switches are the more common switches that can be used to modify the ping command:<br>- **-t** sends ICMP packets until manually stopped.<br>- **-a** resolves addresses to hostnames.<br>- **-n <*count*>** specifies the number of ICMP packets to send. Ping sends 4 packets by default<br>- **-l <*size*>** specifies the packet size in bytes. ping sends 32-byte packets by default |
| tracert/traceroute | The tracert tool shows the path a packet takes to reach its destination. Every device the packet passes through is known as a hop. Use tracert to locate network devices that are down or causing latency issues.<br>- tracert is the Windows version and sends ICMP packets.<br>- traceroute is used in Linux and sends UDP packets. |
| pathping | The pathping Windows command line tool combines the tracert and ping tools. Use pathping to locate network devices that are down or causing latency issues. |
| netstat | Use the netstat command to display a variety of network statistics in both Windows and Linux, including:<br>- Connections for different protocols<br>- Open ports<br>- Running programs |

| | |
|---|---|
| | Some of the common switches used to specify the information shown in Windows are:<br>▪ **-a** displays all connections and listening ports.<br>▪ **-b** displays the executable involved in creating each connection or listening port.<br>▪ **-f** displays the FQDN for the foreign address if possible.<br>▪ **-r** displays the routing table<br>▪ **-p** ***<protocol>*** shows the connections for a specified protocol (TCP, UDP, TCPv6, UDPv6) |
| route | The route command is used in both Windows and Linux to show the routing table and to make manual changes to the table. |
| arp | The arp command is used in both Windows and Linux. ARP stands for Address Resolution Protocol and is used to match IP addresses to MAC addresses. The arp command displays, adds, and removes arp information from network devices. Some of the common switches used with the arp command are:<br>▪ **-a** displays current ARP entries.<br>▪ **inet_addr** specifies an internet address<br>▪ **-d** deletes the host specified by inet_addr |
| nslookup/dig | The nslookup and dig commands are used to view and modify DNS settings. These tools can be used to look up DNS server information and also give IP addresses and domain names for a network server.<br>▪ nslookup is used in Windows.<br>▪ dig is used in Linux. |
| ipconfig/ifconfig | The ipconfig command (Windows) and the ifconfig command (Linux) are used to display the IP configuration on the local computer. Information such as the following can be shown using these commands:<br>▪ Adapter name<br>▪ Adapter MAC address<br>▪ If DHCP is enabled or not<br>▪ IPv6 address<br>▪ IPv4 address<br>▪ Subnet mask<br>▪ IP lease information<br>▪ Default gateway<br>▪ DHCP server<br>▪ DNS server |
| hping | Hping is a security tool that can check connectivity and also analyze the target to gather information. Hping can send ICMP, TCP. UDP, and RAW-IP packets. Hping is primarily designed for Linux but can be installed in Windows. |
| netcat | The netcat security tool can read and write data across both TCP and UDP network connections. It opens a TCP connection between two devices and can be used to send packets, scan for open ports, and listen in on connections to specific ports. You can download netcat from the internet. |
| IP scanners | IP scanners are special tools that allow a network administrator to scan the entire |

| | |
|---|---|
| | network to find all connected devices and their IP addresses. Advanced scans can also display information such as:<br>▪ Routes<br>▪ Hostnames<br>▪ Operating systems |
| nmap | The nmap utility is a network security scanner. Use nmap to scan an entire network or specific IP addresses to discover all sorts of information such as:<br>▪ Open ports<br>▪ Running services<br>▪ Operating system<br>Nmap can use many different protocols and options depending on the network or device being scanned.<br>Nmap is a command line tool, but a GUI version called Zenmap is available. |