1. Small businesses today do need Internet access and use an Internet router to provide this need. A switch is required to connect the two host devices and any IP phones or network devices such as a printer or a scanner. The switch may be integrated into the router. A firewall is needed to protect the business computing assets. Redundancy is not normally found in very small companies, but slightly larger small companies might use port density redundancy or have redundant Internet providers/links.

2. SNMP is a management protocol. TCP is not suitable for the rapid delivery of streaming media. PoE is not a protocol, but a standardized system that allows Ethernet cables to carry power to a device.

3. Capturing traffic during low utilization time will not give a good representation of the different traffic types. Because some traffic could be local to a particular segment, the capture must be done on different network segments.

4. Information theft is the threat by which a company's internal information is accessed and copied by an unauthorized user.

5. One of the most common types of access attack uses a packet sniffer to yield user accounts and passwords that are transmitted as clear text. Repeated attempts to log in to a server to gain unauthorized access constitute another type of access attack. Limiting the number of attempts to log in to the server and using encrypted passwords will help prevent successful logins through these types of access attack.

6. Denial of service attacks involve the disabling or corruption of networks, systems, or services. Reconnaissance attacks are the unauthorized discovery and mapping of systems, services, or vulnerabilities. Access attacks are the unauthorized manipulation of data, system access, or user privileges. Malicious code attacks are computer programs that are created with the intention of causing data loss or damage.

7. The first step is to identify and contain all the infected systems (containment). The systems are then patched (inoculated), disconnected from the network (quarantined), and then cleaned (treatment).

8. Network Address Translation (NAT) translates private addresses into public addresses for use on public networks. This feature prevents outside devices from seeing the actual IP addresses that are used by the internal hosts.

9. Ping round trip time statistics are shown in milliseconds. The larger the number the more delay. A baseline is critical in times of slow performance. By looking at the documentation for the performance when the network is performing fine and comparing it to information when there is a problem, a network administrator can resolve problems faster.

10. An effective network baseline can be established by monitoring the traffic at regular intervals. This allows the administrator to take note when any deviance from the established norm occurs in the network.
11. **Tracert** is used to trace the path a packet takes. The only successful response was from the first device along the path on the same LAN as the sending host. The first device is the default gateway on router R1. The administrator should therefore start troubleshooting at R1.

12. The **show cdp neighbors** command can be used to prove that Layer 1 and Layer 2 connectivity exists between two Cisco devices. For example, if two devices have duplicate IP addresses, a ping between the devices will fail, but the output of **show cdp neighbors** will be successful. The **show cdp neighbors detail** could be used to verify the IP address of the directly connected device in case the same IP address is assigned to the two routers.

13. CDP is a Cisco-proprietary protocol that can be disabled globally by using the **no cdp run** global configuration command, or disabled on a specific interface, by using the **no cdp enable** interface configuration command. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers can learn about each other even if Layer 3 connectivity does not exist. The **show cdp neighbors detail** command reveals the IP address of a neighboring device regardless of whether you can ping the neighbor.

14. To view the contents of NVRAM, the administrator needs to change the current default file system using the **cd** (change directory) command. The **dir** command lists the current directory content of a file system.

15. The startup configuration file is stored in NVRAM, and the running configuration is stored in RAM. The **copy** command is followed by the source, then the destination.

16. WLAN (Wireless Local Area Network). WEP and WPA are security protocols. WPA generates a new dynamic key each time a client establishes a connection with the AP (Access Point)

17. The show version command that is issued on a router displays the value of the configuration register, the Cisco IOS version being used, and the amount of flash memory on the device, among other information.

18. VoIP (Voice over Internet Protocol)

19. The **show file systems** command lists all of the available file systems on a Cisco router. It provides useful information such as the amount of available and free memory of flash and nvram, and its access permissions that include read only (ro), write only (wo), and read and write (rw).

20. The timeout duration for login attempts is set by the **login block-for 180 attempts 4 within 60** command. This command sets the login block at 180 seconds (3 minutes) after 4 incorrect attempts within a 60 second time period. This command can be viewed in the running configuration file.