

## Module Practice and Quiz

1.10.1

### What did I learn in this module?



#### Networks Affect our Lives

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. The creation of the cloud lets us store documents and pictures and access them anywhere, anytime.

#### Network Components

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients. Many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network. An end device is either the source or destination of a message transmitted over the network. Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. The media provides the channel over which the message travels from source to destination.

#### Network Representations and Topologies

Diagrams of networks often use symbols to represent the different devices and connections that make up a network. A diagram provides an easy way to understand how devices connect in a large network. This type of "picture" of a network is known as a topology diagram. Physical topology diagrams illustrate the physical location of intermediary devices and cable installation. Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

#### Common Types of Networks

Small home networks connect a few computers to each other and to the internet. The small office/home office (SOHO) network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources. Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts. The internet is a network of networks that connects hundreds of millions of computers worldwide. The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that spans a small geographical area. A WAN is a network infrastructure that spans a wide geographical area. Intranet refers to a private connection of LANs and WANs that belongs to an organization. An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization's data.

#### Internet Connections

SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone. Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite. The choice of connection varies depending on geographical location and service provider availability. Traditional separate networks used different technologies, rules, and standards. Converged networks deliver data, voice, and video between many different types of devices over the same network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards. Packet Tracer is a flexible software program that lets you use network representations and theories to build network models and explore relatively complex LANs and WANs.

#### Reliable Networks

The term network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network. As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations: Fault Tolerance, Scalability, Quality of Service (QoS), and Security. A fault tolerant network is one that limits the number of affected devices during a failure. Having multiple paths to a destination is known as redundancy. A scalable network expands quickly to support new users and applications. Networks are scalable because the designers follow accepted standards and protocols. QoS is a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network administrators must address two types of network security concerns: network infrastructure security and information security. To achieve the goals of network security, there are three primary requirements: Confidentiality, Integrity, and Availability.

#### Network Trends

There are several recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing. BYOD means any device, with any ownership, used anywhere. Collaboration tools, like Cisco WebEx give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud. There are four primary types of clouds: Public Clouds, Private Clouds, Hybrid Clouds, and Custom Clouds. Smart home technology is currently being developed for all rooms within a house. Smart home technology will become more common as home networking and high-speed internet technology expands. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies. A Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs).

#### Network Security

There are several common external threats to networks:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

These are the basic security components for a home or small office network:

- Antivirus and antispyware
- Firewall filtering

Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

#### The IT Professional

The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures you stay relevant with skill sets needed for the adoption of next-generation technologies. Your CCNA certification will prepare you for a variety of jobs in today's market. At [www.netacad.com](#) you can click the Careers menu and then select Employment opportunities. You can find employment opportunities where you live by using the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

1.10.2

## Module Quiz - Networking Today



1. During a routine inspection, a technician discovered that software that was installed on a computer was secretly collecting data about websites that were visited by users of the computer. Which type of threat is affecting this computer?

- zero-day attack
- DoS attack
- spyware
- identity theft

2. Which term refers to a network that provides secure access to the corporate offices by suppliers, customers and collaborators?

- extranet
- Internet
- intranet
- extendednet

3. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

- cloud computing
- video conferencing
- online collaboration
- bring your own device

4. What is an ISP?

- It is a standards body that develops cabling and wiring standards for networking.
- It is a protocol that establishes how computers within a local network communicate.
- It is an organization that enables individuals and businesses to connect to the Internet.
- It is a networking device that combines the functionality of several different networking devices in one.

5. In which scenario would the use of a WISP be recommended?

- an Internet cafe in a city
- any home with multiple wireless devices
- a farm in a rural area without wired broadband access
- an apartment in a building with cable access to the Internet

6. What characteristic of a network enables it to quickly grow to support new users and applications without impacting the performance of the service being delivered to existing users?

- scalability
- accessibility
- quality of service
- reliability

7. A college is building a new dormitory on its campus. Workers are digging in the ground to install a new water pipe for the dormitory. A worker accidentally damages a fiber optic cable that connects two of the existing dormitories to the campus data center. Although the cable has been cut, students in the dormitories only experience a very short interruption of network services. What characteristic of the network is shown here?

- integrity
- fault tolerance
- security
- scalability
- quality of service (QoS)

8. What are two characteristics of a scalable network? (Choose two.)

- easily overloaded with increased traffic
- grows in size without impacting existing users
- suitable for modular devices that allow for expansion
- is not as reliable as a small network
- offers limited number of applications

9. Which device performs the function of determining the path that messages should take through internetworks?

- a web server
- a router
- a DSL modem
- a firewall

10. Which two Internet connection options do not require that physical cables be run to the building? (Choose two.)

- cellular
- DSL
- dedicated leased line
- dialup
- satellite

11. What type of network must a home user access in order to do online shopping?

- the Internet
- an extranet
- a local area network
- an intranet

12. How does BYOD change the way in which businesses implement networks?

- BYOD requires organizations to purchase laptops rather than desktops.
- BYOD devices are more expensive than devices that are purchased by an organization.
- BYOD provides flexibility in where and how users can access network resources.
- BYOD users are responsible for their own network security, thus reducing the need for organizational security policies.

13. An employee wants to access the network of the organization remotely, in the safest possible way. What network feature would allow an employee to gain secure remote access to a company network?

- IPS
- VPN
- BYOD
- ACL

14. What is the Internet?

- It is a private network for an organization with LAN and WAN connections.
- It provides network access for mobile devices.
- It is a network based on Ethernet technology.
- It provides connections through interconnected global networks.

15. What are two functions of end devices on a network? (Choose two.)

- They provide the channel over which the network message travels.
- They originate the data that flows through the network.
- They direct data over alternate paths in the event of link failures.
- They filter the flow of data to enhance security.
- They are the interface between humans and the communication network.

Check

Show Me

Reset