CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 8

Administering a Secure Network

Objectives

- List and describe the functions of common network protocols
- Explain how network administration principles can be applied
- Define different network applications and how they can be secured

Common Network Protocols

- Protocols
  - Rules for communication
  - Essential for proper communication between network devices
- Transmission Control Protocol/Internet Protocol (TCP/IP)
  - Most common protocol suite used for local area networks and the Internet
  - Comprises several protocols that all function together

Common Network Protocols

- IP
  - Protocol that functions primarily at Open Systems Interconnection (OSI) Network Layer (Layer 3)
  - Provides network addressing and routing
- TCP
  - Transport Layer (Layer 4) protocol
  - Establishes connections and ensures reliable data transport between devices
- TCP/IP uses a four layer architecture
  - Network Interface, Internet, Transport, Application

Common Network Protocols

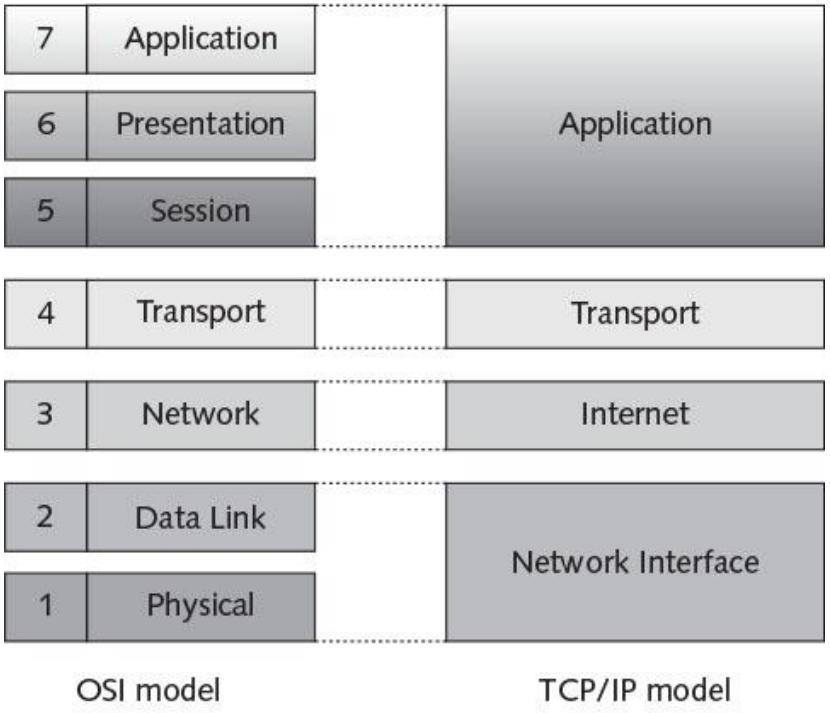

Figure 8-1 OSI model vs. TCP/IP model

Common Network Protocols

- Several basic TCP/IP Protocols:
  - Internet Control Message Protocol (ICMP)
  - Simple Network Management Protocol (SNMP)
  - Domain Name System (DNS)
  - File transfer and storage protocols
  - NetBIOS
  - Telnet
- A new and more secure version of IP is designed to replace the current version

Internet Control Message Protocol (ICMP)

- ICMP
  - Used by devices to communicate updates or error information to other devices
  - ICMP messages are divided into two classes:
    - Informational and query messages
    - Error messages

Internet Control Message Protocol (ICMP)

- ICMP message fields
  - Type
    - Identifies general message category
  - Code
    - Gives additional information about the Type field
  - Checksum
    - Verifies message integrity
  - Message Body
    - Contains information about the specific ICMP message

Internet Control Message Protocol (ICMP)

Type 3 code value	Description
0	Destination network unreachable
1	Destination host unreachable
2	Destination protocol unreachable
3	Destination port unreachable
5	Source route failed
6	Destination network unknown
7	Destination host unknown
9	Communication with destination network administratively prohibited
12	Host unreachable for Type of Service

Table 8-1 Common ICMP code values for Type 3, Destination Unreachable

Internet Control Message Protocol (ICMP)

- Attacks that that advantage of ICMP
  - Network discovery
  - Smurf attack
  - ICMP redirect attack
  - Ping of death

Simple Network Management Protocol (SNMP)

- Used to manage network equipment and is supported by most network equipment manufacturers
- Allows administrators to remotely monitor, manage, and configure network devices
- Functions by exchanging management information between network devices
- Each SNMP-managed device has an agent or a service
  - Listens for and executes commands

Simple Network Management Protocol (SNMP)

- Agents are password protected
  - Password is known as a *community string*
- Security vulnerabilities were present in SMNP versions 1 and 2
  - Version 3 uses usernames and passwords along with encryption to address vulnerabilities

Domain Name System (DNS)

- A TCP/IP protocol that maps IP addresses to their symbolic name
- The DNS database is organized as a hierarchy
  - Database consists of the name of a site and a corresponding IP number
- Database is distributed to many different servers on the Internet
  - To prevent bottlenecking and to ensure efficiency

Domain Name System (DNS)

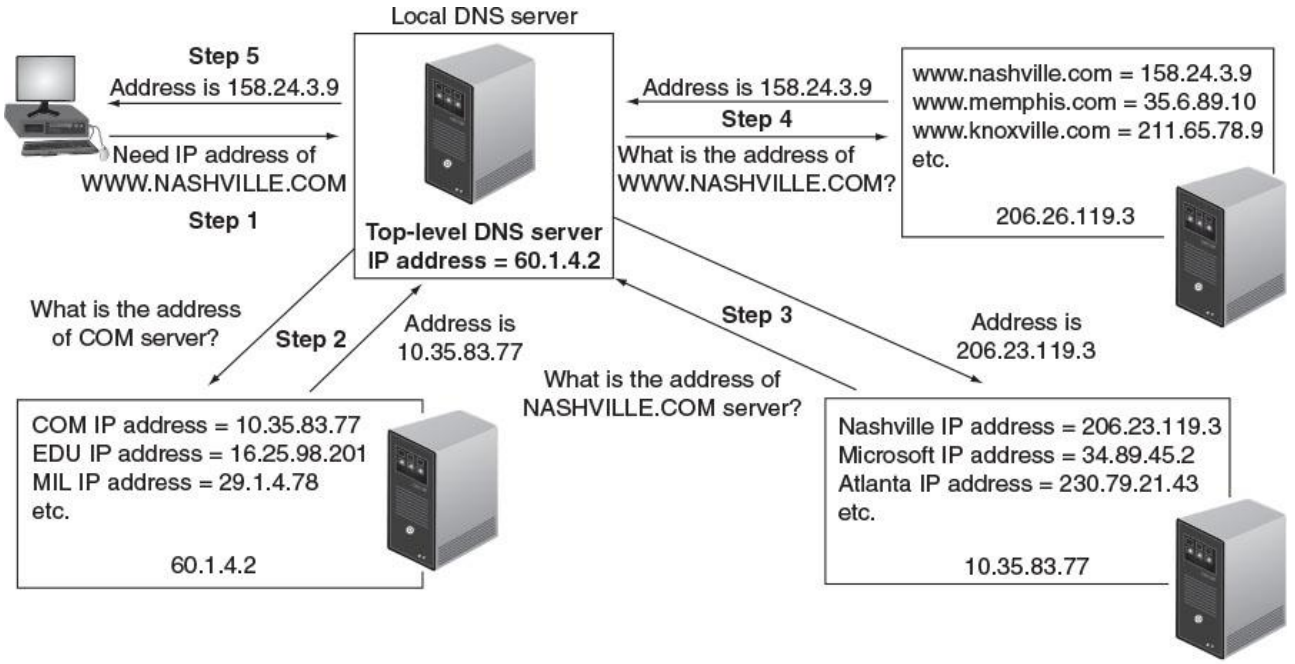

Figure 8-2 DNS lookup

Domain Name System (DNS)

- DNS is often the focus of attacks
  - DNS poisoning substitutes fraudulent IP address
    - Can be done in local host table or external DNS server
    - Latest edition of DNS software prevents DNS poisoning
  - Attacker asks the valid DNS for a zone transfer
    - A zone transfer allows attacker access to network, hardware, and operating system information

File Transfer Protocols

- TCP/IP protocols are used for transferring files
  - File transfer protocol (FTP) - used to connect to an FTP server
  - Trivial file transfer protocol (TFTP) - a “light” version of FTP that uses a small amount of memory
- Methods for using FTP on local host computer
  - *From a command prompt*
  - *Using a web browser*
  - *Using an FTP client*

File Transfer Protocols

- Using FTP behind a firewall can present challenges
  - FTP uses two ports
    - Port 21 is the FTP control part
    - Port 20 is the data port
  - FTP active mode
    - Client's firewall may sometimes drop packets on Port 20 (the data channel connection)
  - FTP passive mode
    - The client sends a PASV command to the command channel and the server responds with the TCP port number to use to establish the data channel

File Transfer Protocols

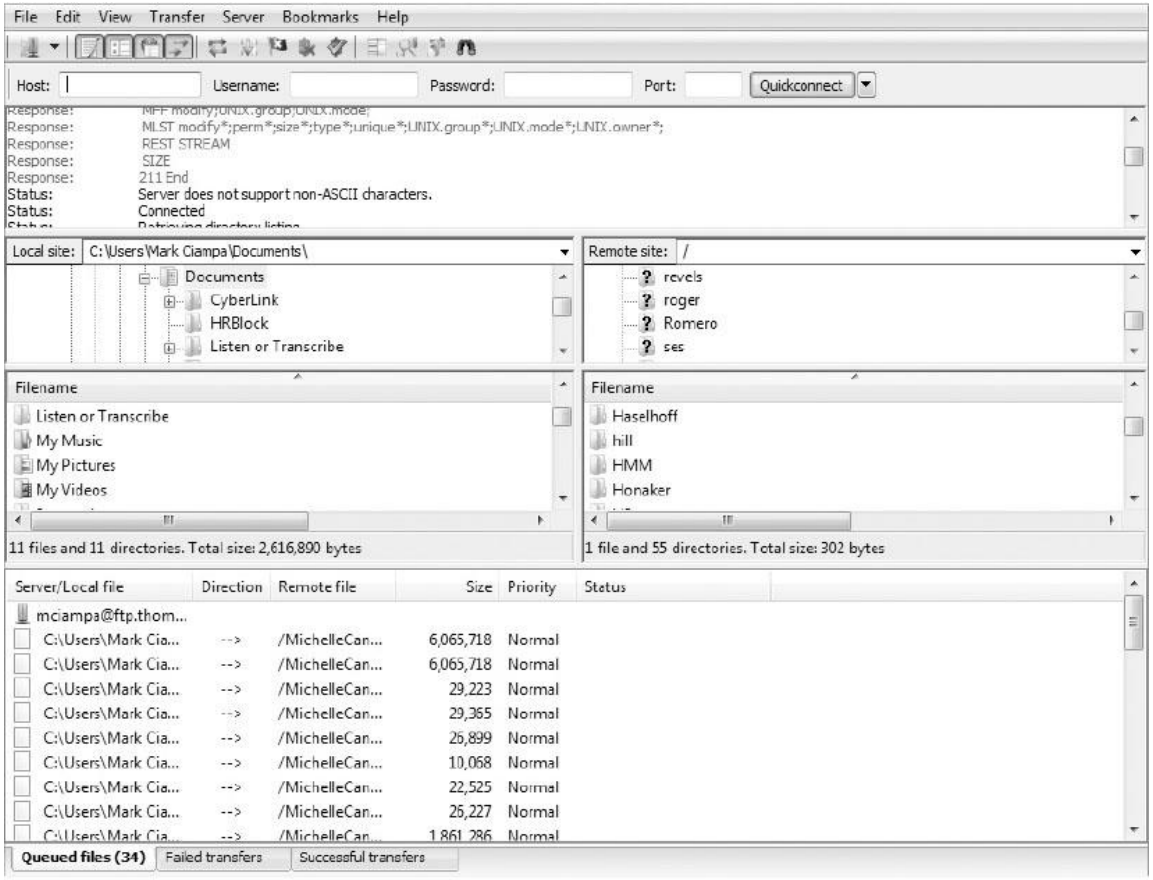

Figure 8-3 FTP client
Source: FileZilla

File Transfer Protocols

- FTP vulnerabilities
  - Does not use encryption
  - Files transferred using FTP are vulnerable to man-in-the-middle attacks
- Secure transmission options over FTP
  - Secure sockets layer (FTPS) encrypts commands
    - Uses SSL or TLS to encrypt commands sent over the control port (port 21); data port may not be encrypted
  - Secure FTP (SFTP)
    - Uses only a single TCP port instead of two ports
    - All data and commands are encrypted

File Transfer Protocols (cont'd.)

- Secure Copy Protocol (SCP)
  - An enhanced version of *Remote Copy Protocol (RCP)*
  - Encrypts files and commands
  - File transfer cannot be interrupted and then resumed in the same session
    - Session must be completely terminated and restarted
  - Found mainly on Linux and UNIX platforms

Storage Protocols

- As storage capacities have grown, most organizations have turned to using a storage area network (SAN)
  - A dedicated network storage facility that provides access to data storage over a high-speed network
- **iSCSI (Internet Small Computer System Interface)** - an IP-based storage networking standard for linking data storage facilities
  - Can transmit data over LANs, WANs, and the Internet

Storage Protocols

- **Fibre Channel (FC)** - a high-speed storage network protocol that can transmit up to 16 Gbps
- **Fibre Channel over Ethernet (FCoE)**
  - A variation of FC that encapsulates Fibre Channel frames over Ethernet networks
  - Allows FC to use fast Ethernet networks while preserving the FC protocol
- FC zones - a built-in security mechanism
  - There are two types:
    - *FC hard zone*
    - *FC soft zone*

NetBIOS

- **NetBIOS (Network Basic Input/Output System)**
  - A transport protocol used by Microsoft Windows systems
  - Allows applications on separate computers to communicate over a LAN
  - An attacker who determines that NetBIOS is running can use an application to gather information regarding the network in order to design an attack
  - It is recommended to disable NetBIOS or used only if necessary on specific devices that require it

Telnet

- **Telnet**
  - An older TCP/IP protocol for text-based communication
  - Also a terminal emulation application that runs on a local computer
    - Connects to a server on a network
  - Telnet does not encrypt data and many security weaknesses have been uncovered within the protocol
  - It is recommended that Secure Shell (SSH) be used instead of Telnet

Network Administration Principles

- Administering a secure network can be challenging
- Rule-based management approach
  - Relies on following procedures and rules
  - Procedural rules are the authoritative and prescribed direction for conduct
    - Procedural rules dictate technical rules
  - Technical rules address:
    - Device security
    - Monitoring and analyzing logs
    - Network design management
    - Port security

Device Security

- Device security involves:
  - Establishing a secure router configuration
  - Implementing flood guards
- Secure router configuration
  - Router operates at Network Layer (Layer 3)
    - Forwards packets across computer networks
  - Routers can perform a security function
    - Can be configured to filter out specific types of network traffic

Device Security

Task	Explanation
Create a network design	Prior to any configuration, a network diagram that illustrates the router interfaces should be created. This diagram should reflect both the LAN and wide area network (WAN) interfaces.
Use a meaningful router name	Because the name of the router appears in the command line during router configuration, it helps ensure that commands are given to the correct router. For example, if the name *Internet_Router* is assigned to the device, the displayed command prompt would be *Internet_Router (config)#*.
Secure all ports	All ports to the router should be secured. This includes both physical ports (sometimes called the *console port* and *auxiliary port*) and inbound ports from remote locations (sometimes known as *VTY* for *virtual teletype*).
Set a strong administrator password	Most routers allow a user to access the command line in *user mode*, yet an administrator password is required to move to *privileged mode* for issuing configuration commands.
Make changes from the console	The configuration of the router should be performed from the console and not a remote location. This configuration can then be stored on a secure network drive as a backup and not on a laptop or USB flash drive.

Table 8-4 Secure router configuration tasks

Device Security

- Flood guard
  - Protects against denial of service (DoS) attacks
  - SYN flood attack
    - A type of DoS attack that takes advantage of the procedures for initiating a session
  - A flood guard controls a device's tolerance for unanswered service requests
    - Administrator can set a maximum number of "developing" connections
  - Commonly found on firewalls, IDSs, and IPSs

Monitoring and Analyzing Logs

- Security logs
  - Can reveal types of attacks that are being directed at the network and if attacks were successful
- Access logs
  - Provide details regarding requests for specific files
- Audit logs
  - Used to record which user performed an action
- Event logs
  - Document any unsuccessful events and the most significant successful events

Monitoring and Analyzing Logs

- A routine review of logs helps to:
  - Identify security incidents
  - Policy violations
  - Fraudulent activity
  - Operational problems
- Logs can be useful for:
  - Performing auditing analysis
  - Supporting the organization's internal investigations
  - Identifying operational trends and long-term problems

Monitoring and Analyzing Logs

- Logs can provide documentation that the organization is complying with laws and regulatory requirements
- Firewall log items to be examined
  - IP addresses rejected and dropped
  - Probes to ports that have no application services on them
  - Source-routed packets
  - Suspicious outbound connections
  - Unsuccessful logins

Monitoring and Analyzing Logs

Device	Explanation
Firewalls	Firewall logs can be used to determine whether new IP addresses are attempting to probe the network and if stronger firewall rules are necessary to block them. Outgoing connections, incoming connections, denied traffic, and permitted traffic should all be recorded.
Network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS)	Intrusion detection and intrusion prevention systems record detailed security log information on suspicious behavior as well as any attacks that are detected. In addition, these logs also record any actions NIPS used to stop the attacks.
Web servers	Web servers are usually the primary target of attackers. These logs can provide valuable information about the type of attack that can help in configuring good security on the server.
DHCP servers	DHCP server logs can identify new systems that mysteriously appear and then disappear as part of the network. They can also show what hardware device had which IP address at a specific time.
VPN concentrators	VPN logs can be monitored for attempted unauthorized access to the network.
Proxies	As intermediate hosts through which websites are accessed, these devices keep a log of all URLs that are accessed through them. This information can be useful when determining if a zombie is "calling home."
Domain Name System (DNS)	A DNS log can create entries in a log for all queries that are received. Some DNS servers also can create logs for error and alert messages.
Email servers	Email servers can show the latest malware attacks that are being launched through the use of attachments.
Routers and switches	Router and switch logs provide general information about network traffic.

Table 8-5 Device logs with beneficial security data

Monitoring and Analyzing Logs

- Problems with log management:
  - Multiple devices generating logs
  - Very large volumes of data
  - Different log formats
- A solution to log management is to use a centralized device log analyzer

Network Design Management

- Several network design management principles should be followed to ensure a secure network
- Network separation
  - Provides separation between different parts of the network
  - Example: order entry network segment cannot access the network that controls heating and cooling
- Option to accomplish network separation
  - Physically separate users by connecting them to different switches and routers

Network Design Management

- Loop protection
  - Refer to Figure 8-7 for a description of a broadcast storm
  - Host Z wants to send frames to Host X
  - Switch A floods network with the packet
  - Packet travels down the network segments to the Switches B and C
  - Switches B and C add Host Z to their lookup tables
  - Both switches flood Segment 2 looking for Host X
    - They receive each other's packets and flood them back out again

Network Design Management

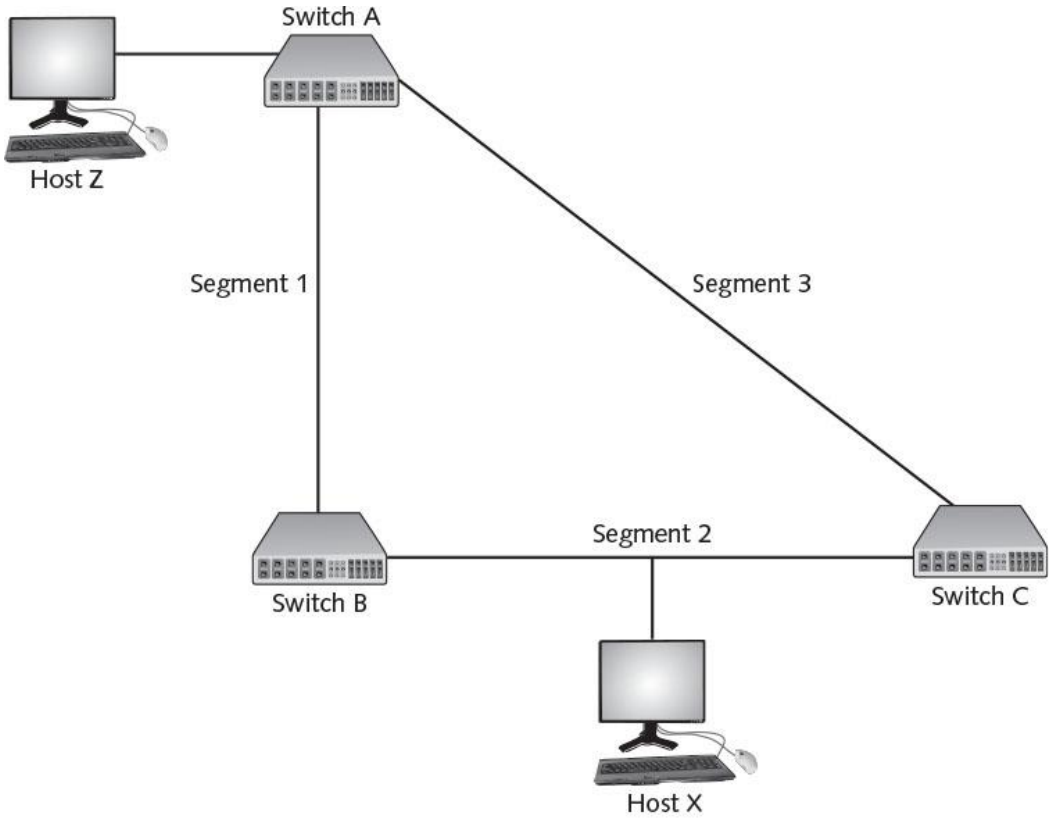

Figure 8-7 Broadcast storm

Network Design Management

- Loop protection can prevent broadcast storms
  - Uses IEEE 802.1d *spanning tree algorithm (STA)*
  - Determines which switch has multiple ways to communicate with host
  - Determines best path and blocks other paths
- Virtual LAN (VLAN) management
  - Network may be segmented into logical groups of physical devices through VLAN
  - Scattered users may be logically grouped together:
    - Regardless of which switch they are attached to

Network Design Management

- General principles for managing VLANs
  - Configure empty switch ports to connect to an unused VLAN
  - Change any default VLAN names
  - Configure the ports on the switches that pass tagged VLAN packets to explicitly forward specific tags
  - Configure VLANs so that public devices are not on a private VLAN

Port Security

- Disabling unused interfaces
  - Turn off ports not required on a network device that are not required
  - A switch or router without port security allows attackers to connect to unused ports and attack the network
  - All interfaces should be secured before switch is deployed
  - The network administrator should issue shutdown command to each unused port

Securing Network Applications and Platforms

- Several network applications and platforms require special security considerations:
  - IP telephony
  - Virtualization
  - Cloud computing

IP Telephony

- A shift to an all digital technology infrastructure is underway
  - Converges voice and data traffic over a single IP network
  - IP telephony adds digital voice clients and new voice applications to a data based network
- An IP telephony application can be easily developed that personalizes the treatment of incoming calls
  - Calls can be selectively forwarded or blocked

Virtualization

- Virtualization
  - A means of managing and presenting computer resources without regard to physical layout or location
- Host virtualization
  - An entire operating system environment is simulated
  - Virtual machine - a simulated software-based emulation of a computer
  - The host system runs a hypervisor that manages the virtual operating systems and supports one or more guest systems

Virtualization

- Virtualization advantages
  - New virtual server machines can be made available (host availability) and resources can easily be expanded or contracted as needed (host elasticity)
  - Can reduce costs
    - Fewer physical computers must be purchased and maintained
  - Can provided uninterrupted server access to users
    - Supports *live migration* which allows a virtual machine to be moved to a different physical computer with no impact to users

Virtualization

- Virtualization advantages (cont'd.)
  - Test latest patches by downloading on a virtual machine before installing on production computers
  - A snapshot of a particular state of a virtual machine can be saved for later use
  - Testing the existing security configuration (**security control testing**) can be performed using a simulated network environment
  - A suspicious program can be loaded into an isolated virtual machine and executed (**sandboxing**)
    - If malware, only the virtual machine will be impacted

Cloud Computing

- Cloud computing
  - A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
  - It is a pay-per-use computing model
    - Customers pay for only the resources they need
- Types of clouds
  - Public cloud
  - Community cloud
  - Private cloud
  - Hybrid cloud

Cloud Computing

- Three service models of cloud computing
  - **Software as a Service (SaaS)**
    - Vendor provides access to the vendor's software applications running on a cloud infrastructure
  - **Platform as a Service (PaaS)**
    - Consumers install and run their own specialized applications on the cloud computing network
  - **Infrastructure as a Service (IaaS)**
    - Vendor allows customers to deploy and run their own software, including OSs and applications

Summary

- TCP/IP is the most common protocol for LANs and the Internet
- Protocols for transferring files
  - FTP, FTPS, SFTP, SCP
- Storage area network (SAN) is a dedicated network storage facility that provides access to data storage over a high-speed network
- Router configuration must provide a secure network environment
- Flood guard defends against denial-of-service attacks

Summary

- Networks can be configured to provide separation and increased security
- Securing ports is an important step in network management
  - Unused ports should be disabled
- New network applications that have special security considerations
  - IP telephony
  - Virtualization
  - Cloud computing