Objectives

• List and describe the functions of common network protocols
• Explain how network administration principles can be applied
• Define the new types of network applications and how they can be secured
Common Network Protocols

• Protocols
  – Rules of conduct and 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
Common Network Protocols (cont’d.)

- **IP**
  - Protocol that functions primarily at Open Systems Interconnection (OSI) Network Layer (Layer 3)

- **TCP**
  - Transport Layer (Layer 4) protocol
  - Establishes connections and reliable data transport between devices

- **TCP/IP uses a four layer architecture**
  - Network Interface, Internet, Transport, Application
Figure 7-1 OSI model vs. TCP/IP model

© Cengage Learning 2012
Internet Control Message Protocol (ICMP)

- ICMP
  - One of the core protocols of TCP/IP
  - Used by devices to communicate updates or error information to other devices
  - Used to relay query messages
Internet Control Message Protocol (cont’d.)

• ICMP message fields
  – Type (8-bit)
    • Identifies general message category
  – Code (8-bit)
    • Gives additional information about the Type field
  – Checksum (16-bit)
    • Verifies message integrity
<table>
<thead>
<tr>
<th>Type 3 code value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Network unreachable</td>
</tr>
<tr>
<td>1</td>
<td>Host unreachable</td>
</tr>
<tr>
<td>2</td>
<td>Protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Port unreachable</td>
</tr>
<tr>
<td>5</td>
<td>Source route failed</td>
</tr>
<tr>
<td>6</td>
<td>Destination network unknown</td>
</tr>
<tr>
<td>7</td>
<td>Destination host unknown</td>
</tr>
<tr>
<td>9</td>
<td>Communication with destination network administratively prohibited</td>
</tr>
<tr>
<td>12</td>
<td>Host unreachable for type of service</td>
</tr>
</tbody>
</table>

Table 7-1 Common ICMP code values for Type 3, Destination Unreachable
Internet Control Message Protocol (cont’d.)

• Attacks that use ICMP
  – Network discovery
  – Smurf DoS attack
  – ICMP redirect attack
  – Ping of death
Simple Network Management Protocol (SNMP)

- First introduced in 1988
- 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 service
  - Listens for and executes commands
Simple Network Management Protocol (cont’d.)

• Agents are password protected
  – Password is known as community string

• Security vulnerabilities were present in SMNP versions 1 and 2
  – Version 3 introduced in 1998
  – Uses usernames and passwords along with encryption to address vulnerabilities
Domain Name System (DNS)

- DNS
  - A TCP/IP protocol that maps IP addresses to their symbolic name
  - Database with name of each site and corresponding IP number
  - Database is distributed to many different servers on the Internet
Figure 7-2 DNS lookup
© Cengage Learning 2012
Domain Name System (cont’d.)

• DNS can be 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
  – Zone transfer allows attacker access to network, hardware, and operating system information
File Transfer Protocols

• TCP/IP protocols used for transferring files
  – File transfer protocol (FTP)
  – Secure transfer protocol (SCP)
• Methods for using FTP on local host computer
  – Command prompt
  – Web browser
  – FTP client
• Using FTP behind a firewall can present challenges
  – FTP active mode
  – FTP passive mode
Figure 7-3 FTP client
© Cengage Learning 2012
File Transfer Protocols (cont’d.)

• FTP vulnerabilities
  – Does not use encryption
  – Files transferred using FTP vulnerable to man-in-the-middle attacks

• Secure transmission options over FTP
  – Secure sockets layer (FTPS) encrypts commands
  – Secure FTP (SFTP)
File Transfer Protocols (cont’d.)

• Secure Copy Protocol (SCP)
  – Enhanced version of Remote Copy Protocol
  – Encrypts files and commands
  – File transfer cannot be interrupted and resumed
  – Found mainly on Linux and UNIX platforms
IPv6

• Current version of IP protocol is version 4 (IPv4)
  – Developed in 1981
  – Number of available IP address is limited to 4.3 billion
    • Number of internet connected devices will grow beyond this number
  – Has security weaknesses
• Internet Protocol version 6 (IPv6)
  – Next generation of IP protocol
  – Addresses weaknesses of IPv4
Figure 7-4 IPv4 and IPv6 headers
© Cengage Learning 2012
IPv6 (cont’d.)

• IPv6 (cont’d.)
  – Provides enhanced security features
    • Cryptographic protocols
    • New authentication headers prevent IP packets from being altered
<table>
<thead>
<tr>
<th>IPv4 field name</th>
<th>IPv6 field name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Header Length (IHL)</td>
<td>[Not used]</td>
<td>IPv6 uses a fixed packet header size of 40 bytes, so information always appears in the same place. This is a much smaller header size than IPv4 because packets only contain the header information that they need; the smaller size speeds up finding information in the packet and processing the packet</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Traffic class</td>
<td>Currently, there no standard requirements for the content of this field</td>
</tr>
<tr>
<td>[Not used]</td>
<td>Flow label</td>
<td>Packets belonging to the same stream, session, or flow share a common flow value, making it more easily recognizable without looking deeper into the packet</td>
</tr>
<tr>
<td>Total length</td>
<td>Payroll length</td>
<td>Payroll Length, which includes any additional headers, no longer includes the length of the header (as in IPv4), so the host or router does not need to check if the packet is large enough to hold the IP header</td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td>Hop limit</td>
<td>TTL was a misnomer because it never contained an actual time value</td>
</tr>
<tr>
<td>Protocol</td>
<td>Next header</td>
<td>This indicates the type of header that follows</td>
</tr>
<tr>
<td>Source address and destination address</td>
<td>Source address and destination address</td>
<td>These serve the same function in IPv6 except they are expanded from 32 bits to 128 bits</td>
</tr>
</tbody>
</table>

Table 7-2 Comparison of IPv4 and IPv6 headers
Network Administration Principles

- Administering a secure network can be challenging
- Rule-based management approach
  - Relies on following procedures and rules
  - Rules may be external (applicable laws) or internal
  - Procedural rules dictate technical rules
  - Technical rules
    - Device security
    - Network management and port security
    - Example: configuring a firewall to conform to procedural rules
Device Security

• Device security
  – Establishing a secure router configuration
  – Implementing flood guards
  – Analyzing device logs
• 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
<table>
<thead>
<tr>
<th>Task</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a design</td>
<td>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, as illustrated in Figure 7-5</td>
</tr>
<tr>
<td>Use a meaningful router name</td>
<td>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, then the displayed command prompt would be Internet_Router (config)#</td>
</tr>
<tr>
<td>Secure all ports</td>
<td>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)</td>
</tr>
<tr>
<td>Set a strong administrator password</td>
<td>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</td>
</tr>
<tr>
<td>Make changes from the console</td>
<td>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</td>
</tr>
</tbody>
</table>

Table 7-3 Secure router configuration tasks
Figure 7-5 Network diagram showing routers
© Cengage Learning 2012
Device Security (cont’d.)

- **SYN flood attack**
  - Takes advantage of procedures for initiating a session
- **Flood guard**
  - Protects against denial of service attacks
  - Controls device’s tolerance for unanswered service requests
    - Set maximum number of “developing” connections
  - Commonly found on firewalls, IDSs, and IPSs
Device Security (cont’d.)

• Log analysis
  – Log records events that occur
  – Monitoring logs can be useful in determining how attack occurred
  – System logs and security application logs
  – Network security logs

• Types of security hardware logs
  – NIDS, NIPS, DNS, proxy servers, and firewalls
<table>
<thead>
<tr>
<th>Type of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification messages from other servers</td>
</tr>
<tr>
<td>Dynamic updates</td>
</tr>
<tr>
<td>Content of the question section for DNS query messages</td>
</tr>
<tr>
<td>Content of the answer section for DNS query messages</td>
</tr>
<tr>
<td>Number of queries this server sends</td>
</tr>
<tr>
<td>Number of queries this server has received</td>
</tr>
<tr>
<td>Number of DNS requests received over a TCP port</td>
</tr>
<tr>
<td>Number of full packets sent by the server</td>
</tr>
<tr>
<td>Number of packets written through by the server and back to the zone</td>
</tr>
</tbody>
</table>

Table 7-4 DNS detailed log data
Outgoing Log Table

<table>
<thead>
<tr>
<th>LAN IP</th>
<th>Destination URL/IP</th>
<th>Service/Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.136</td>
<td>161.6.18.93</td>
<td>https</td>
</tr>
<tr>
<td>192.168.1.136</td>
<td>207.115.11.17</td>
<td>pop3</td>
</tr>
<tr>
<td>192.168.1.136</td>
<td>207.115.11.17</td>
<td>smtp</td>
</tr>
<tr>
<td>192.168.1.136</td>
<td>207.115.11.17</td>
<td>pop3</td>
</tr>
</tbody>
</table>

Figure 7-6 Basic firewall log
© Cengage Learning 2012
Figure 7-7 Detailed firewall log
© Cengage Learning 2012
Device Security (cont’d.)

• Firewall log items to be examined
  – IP addresses rejected and dropped
  – Probes to ports that have no application servers on them
  – Source-routed packets
  – Suspicious outbound connections
  – Unsuccessful logins
Network Design Management

- Growing network may need reconfiguration
- Network separation
  - Provides separation between different parts of the network
  - Example: order entry network segment cannot access human resources network
- Options to accomplish network separation
  - Physically separate users by connecting them to different switches and routers
  - Air gap switch
Network Design Management (cont’d.)

• Loop protection
  – Refer to Figure 7-8 for description of broadcast storm
  – Host Z wants to send frames to Host X
  – Switch A floods network with the packet
  – Packet travels down Segments 1 and 3 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
Figure 7-8 Broadcast storm
© Cengage Learning 2012
Network Design Management (cont’d.)

• Loop protection can prevent broadcast storms
  – Uses IEEE 802.1d spanning tree algorithm
  – 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 (cont’d.)

• General principles for managing VLANs
  – A VLAN should not communicate with another VLAN unless they are both connected to a router
  – Configure empty switch ports to connect to an unused VLAN
  – Different VLANs should be connected to different switches
  – Change any default VLAN names
Network Design Management (cont’d.)

- General principles for managing VLANs (cont’d.)
  - Configure switch ports 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 ports
  - Turn off ports not required on a network
  - Often overlooked security technique
  - Switch without port security allows attackers to connect to unused ports and attack network
  - All ports should be secured before switch is deployed
  - Network administrator should issue shutdown command to each unused port
Port Security (cont’d.)

• MAC limiting and filtering
  – Filters and limits number of media access control (MAC) addresses allowed on a port
  – Port can be set to limit of 1
  – Specific MAC address can be assigned to a port
    • Enables only single authorized host to connect
<table>
<thead>
<tr>
<th>Configuration setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>The MAC addresses are manually entered and then stored on the device</td>
</tr>
<tr>
<td>Dynamic</td>
<td>The MAC addresses are automatically learned and stored; when the switch restarts, the settings are erased</td>
</tr>
<tr>
<td>Sticky</td>
<td>The MAC addresses are automatically learned and stored along with any addresses that were learned prior to using the Sticky configuration; if this configuration is disabled, the addresses are kept in memory yet are removed from the table</td>
</tr>
</tbody>
</table>

Table 7-5 MAC limiting and filtering configuration options
Port Security (cont’d.)

• IEEE 802.1x
  – Standard that provides the highest degree of port security
  – Implements port-based authentication
  – Blocks all traffic on a port-by-port basis:
    • Until client is authenticated
Figure 7-9 IEEE 802.1x process
© Cengage Learning 2012
Securing Network Applications

• Virtualization
  – Means of managing and presenting computer resources without regard to physical layout or location

• Operating system virtualization
  – Virtual machine simulated as software environment on host system

• Virtualization advantages
  – Test latest patches by downloading on a virtual machine before installing on production computer
Securing Network Applications (cont’d.)

• Virtualization advantages (cont’d.)
  – Penetration testing can be performed using simulated network environment
  – Can be used for training purposes

• Server virtualization
  – Creating and managing multiple server operating systems
  – Relies on the hypervisor software to manage virtual operating systems
  – Can reduce costs and energy use
Securing Network Applications (cont’d.)

• Server virtualization (cont’d.)
  – Can help provide users uninterrupted server access
  – Live migration enables virtual machine to be moved to a different computer with no user impact
    • Can also be used for load balancing

• Virtualized environment security concerns
  – Physical firewall may not be able to inspect and filter amount of traffic coming from running multiple virtualized servers
Securing Network Applications (cont’d.)

- Virtualized environment security concerns (cont’d.)
  - Security must be in place to accommodate live migration
  - Some hypervisors do not have necessary security controls to keep out attackers
  - Existing security tools do not always adapt well to multiple virtual machines
  - External physical appliances not designed to protect multiple virtual servers
  - Virtual machines need protection from other virtual machines running on the same computer
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic protection</td>
<td>Anti-virus, firewall, and IDS features protect virtualized servers</td>
</tr>
<tr>
<td>Restrict changes</td>
<td>Users cannot stop or change the configuration of a virtual machine</td>
</tr>
<tr>
<td>Auditing</td>
<td>Logs can automatically be scanned to determine if any changes were made</td>
</tr>
<tr>
<td>Compliance</td>
<td>Selecting a specific set of guidelines can generate 30 or more automatic hardening procedures, such as securing SNMP access and enforcing minimum password requirements</td>
</tr>
<tr>
<td>Customization</td>
<td>Different security zones can be created for different virtualized servers</td>
</tr>
<tr>
<td>Reporting</td>
<td>Visual maps of which guests are running on which hosts along with network traffic patterns and the amount of disk storage attached can be generated</td>
</tr>
</tbody>
</table>

Table 7-6 Virtualization security tool features
IP Telephony

• Shift to all digital technology infrastructure is underway
  – Converges voice and data traffic over single IP network
  – IP telephony adds digital voice clients and new voice applications to a data based network

• IP telephony advantages
  – Incoming calls can be selectively forwarded or blocked
IP Telephony (cont’d.)

- IP telephony advantages (cont’d.)
  - Cost savings
  - Managing a single network for all applications
  - Applications can be developed more quickly with fewer resources
  - Reduced wired infrastructure requirements
  - Reduced regulatory requirements
  - Increased user productivity
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating systems</td>
<td>“Softphones” that operate on standard PCs are vulnerable to operating system attacks</td>
</tr>
<tr>
<td>VoIP protocols</td>
<td>Many of the common VoIP protocols do not provide adequate call-party authentication, end-to-end integrity protection, and confidentiality measures</td>
</tr>
<tr>
<td>Lack of encryption</td>
<td>Voice protocols do not encrypt call-signaling and voice streams, so identities, credentials, and phone numbers of callers can be captured using protocol analyzers</td>
</tr>
<tr>
<td>Network acknowledgment</td>
<td>Attackers can flood VoIP targets with DoS-type attacks that can degrade service, force calls to be dropped prematurely, and render certain VoIP equipment incapable of processing calls</td>
</tr>
<tr>
<td>Spam</td>
<td>Spam over Internet telephony can carry unsolicited sales calls and other nuisance messages, and programs can download hidden malware to softphones</td>
</tr>
</tbody>
</table>

Table 7-7 IP telephony vulnerabilities
Cloud Computing

• Pay-per-use computing model
  – Customers pay for only the resources they need
  – May revolutionize computing
  – Unlike hosted services, does not require long-term contracts

• Three service models of cloud computing
  – Cloud software as a service (SaaS)
  – Cloud platform as a service (PaaS)
  – Cloud infrastructure as a service (IaaS)
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-demand self-service</td>
<td>The consumer can automatically increase or decrease computing resources without requiring any human interaction from the service provider</td>
</tr>
<tr>
<td>Universal client support</td>
<td>Virtually any networked device (desktop, laptop, smartphone, pad, and so on) can access the cloud computing resources</td>
</tr>
<tr>
<td>Invisible resource pooling</td>
<td>The physical and virtual computing resources are pooled together to serve multiple, simultaneous consumers that are dynamically assigned or reassigned according to the consumer’s needs; the customer has little or no control or knowledge of the physical location of the resources</td>
</tr>
<tr>
<td>Immediate elasticity</td>
<td>Computing resources are “elastic” in that they can be increased or decreased quickly to meet demands</td>
</tr>
<tr>
<td>Metered services</td>
<td>Fees are based on the computing resources used</td>
</tr>
</tbody>
</table>

Table 7-8 Cloud computing characteristics
Cloud Computing (cont’d.)

• Cloud computing security challenges
  – Cloud provider must guarantee means to approve authorized users and deny imposters
  – Transmissions from the cloud must be protected
  – Customers’ data must be isolated from one another
Summary

• TCP/IP
  – Most common protocol for LANs and the Internet
• Protocols for transferring files
  – FTP, FTPS, SFTP, SCP
• Router configuration must provide a secure network environment
• Flood guard defends against denial-of-service attacks
• Networks can be configured to provide separation and increased security
Summary (cont’d.)

• Securing ports is an important step in network management
  – Unused ports should be disabled
• New network applications that have special security considerations
  – Virtualization
  – IP telephony
  – Cloud computing