Technology in Action

Alan Evans • Kendall Martin
Mary Anne Poatsy

Tenth Edition
Chapter 10
Behind the Scenes:
Networking and Security in the Business World
Chapter Topics

• Client/Server Networks and Topologies
  – Basics of Client/Server Networks
  – Servers and Network Topologies
• Setting Up Business Networks
  – Transmission Media
  – Network Adapters and Network Navigation Devices
  – Network Operating Systems
  – Network Security for Client/Server Networks
Basics of Client/Server Networks

• A network is group of two or more computing devices (nodes)
• Share information and resources
  – Printers
  – Files
  – Databases
• Businesses gain advantages from deploying networks
Basics of Client/Server Networks

Networking Advantages

• Advantages businesses gain from networks
  – Enable sharing of expensive resources
  – Facilitate knowledge sharing
    • Serve needs of many people at one time
    • Increase availability of data
  – Enable sharing of software
  – Enable enhanced communication
Basics of Client/Server Networks

Networking Advantages

Benefits of Business Networks

Enable resource sharing
- Expensive peripherals, such as printers, can be shared
- Networks can share a single internet connection

Facilitate knowledge sharing
- Data can be accessed by multiple people

Enable software sharing
- Software can be delivered to client computers from a server

Enhance communication
- Information sharing is more effective when employees are connected
• Disadvantages to using networks
  – Additional personnel are usually required to maintain network
    • Network administrators
    • Trained in computer maintenance
    • Design networks
    • Install networking software
  – Requires special equipment and software
  – Cost savings and advantages outweigh cost and disadvantages
Where to find client/server networks

- Majority of computer networks are client/server
  - Server stores and shares resources on a network
  - Client requests resources
- Tasks can be handled centrally at the server
  - Backups of data files
  - Coordination of security
- Client/server is considered centralized
- Peer-to-peer (P2P) is decentralized
Basics of Client/Server Networks
Comparing Client/Server and Peer-to-Peer Networks (cont.)

• Why businesses use client/server networks
  – Makes data flow more efficiently than P2P
  – Responds to requests from large number of clients at the same time
  – Can be configured to perform specific tasks efficiently
    • E-mail
    • Database requests
Why P2P networks aren’t used more in business settings

- Difficult to administer beyond 10 users
- Inefficient with large number of computers
- Security can’t be implemented centrally
- Client computers are more efficient at processor-intensive tasks

- Viewing a video
- Accessing a database
• Making a client/server network different from a P2P network
  – Increased scalability
    • More users can be added easily
    • Doesn’t affect the performance of other nodes
    • Can be done without disrupting existing users
Basics of Client/Server Networks

Types of Client/Server Networks

• The most common types of client/server networks encountered in businesses
  – Local area network (LAN)
    • Small group of computers and peripherals
    • Relatively small geographic area
  – Wide area network (WAN)
    • Large number of users
    • Wider physical area
    • Separate LANs that are miles apart
### Classifications of Client/Server Networks

<table>
<thead>
<tr>
<th>NETWORK TYPE</th>
<th>DESCRIPTION</th>
<th>WHERE USED IN BUSINESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAN (Personal Area Network)</td>
<td>Devices used by one person connected via wireless media</td>
<td>Usually by employees traveling on business</td>
</tr>
<tr>
<td>LAN (Local Area Network)</td>
<td>A network consisting of nodes covering a small geographic area</td>
<td>In small businesses or self-contained units of a large business (such as one or more floors of the same office building)</td>
</tr>
<tr>
<td>HAN (Home Area Network)</td>
<td>A type of small LAN installed in a home</td>
<td>Not usually deployed by businesses, except small home-based businesses</td>
</tr>
<tr>
<td>WAN (Wide Area Network)</td>
<td>Two or more LANs connected together, often over long distances</td>
<td>Connecting business LANs over long distances such as between branches in two cities</td>
</tr>
<tr>
<td>MAN (Metropolitan Area Network)</td>
<td>WANs constructed by municipalities to provide connectivity in a specific geographic area</td>
<td>Although not deployed by businesses, employees often use them while traveling</td>
</tr>
</tbody>
</table>
Basics of Client/Server Networks

Types of Client/Server Networks (cont.)

• Other networks businesses use
  – Intranet
    • Private network used exclusively by select group
    • Facilitate information sharing
    • Not accessible by unauthorized people
  – Extranet
    • Area of intranet with limited access
    • Useful for electronic data interchange (EDI)
      – EDI allows the exchange of large amounts of business data in a standardized electronic format
How Virtual Private Networks keep information secure on intranets and extranets

- Use public communications infrastructure to build a secure networks among locations
- Can used leased line, but these are expensive
- Use special security technologies and protocols to enhance security
- Requires special hardware and software
• How VPNs work using tunneling
  – Data packets are placed into other data packets
  – Encrypted so only understood by sending and receiving hardware (tunnel interface)
  – Hardware is optimized to seek efficient routes of transmission
  – Provides a high level of security
Basics of Client/Server Networks

Types of Client/Server Networks (cont.)
The key components of a client/server network

- Servers
- Network topologies
- Transmission media
- Network adapters
- Network navigation devices
- Network operating system
Basics of Client/Server Networks
Types of Client/Server Networks (cont.)
Servers

- Servers found on larger client/server networks
  - Dedicated server
    - Fulfill one specific function
    - Additional servers can be added to reduce load on main server
    - Can allow the original server to become a dedicated server
Servers (cont.)

- Functions dedicated servers handle
  - Repetitive tasks
  - Demand a lot of processor (CPU) time
- Common servers
  - Authentication servers
  - Print servers
  - Database servers
  - Communications servers
  - Cloud servers
  - File servers
  - Application servers
  - E-mail servers
  - Web servers
Servers (cont.)
Servers
Authentication and File Servers

• Authentication servers
  – Keep track of who is logging on to the network
  – Keep track of which services are available to each user
  – Act as overseers for the network
  – Manage and coordinate services provided by dedicated servers

• File servers
  – Store and manage files for network users
How a print server functions

- Manages all client-requested printing jobs
- Helps client computers be more productive by relieving them of printing duties
- Frees up the CPU on client computer to do other jobs
• How the printer knows which documents to print
  – Print queue (print spooler) is a holding area for print jobs
  – Each printer has its own named print queue
  – Print jobs receive a number and go to the printer in the order in which they were received
  – Queue can be set to prioritize jobs
Servers

Application Servers

• Functions an application server performs
  – Acts as a repository for application software
  – Delivers the software when a client computer makes a request
  – Eases installation and upgrading
  – Application is installed or upgraded only on application server
• What a database server does
  – Provides clients with information stored in databases
  – Makes it possible for many people to access the database at one time
  – Database resides only on the database server
Servers
E-Mail Servers

• How e-mail is handled on a large client/server network
  – Processes and delivers incoming and outgoing e-mail
  – Large volume could overwhelm a server that handled other tasks
  – Handles the routing and delivery of the message
Servers
Communications Servers

• Types of communications a communications server handle
  – Handles all communications between the network and other networks
  – Manages Internet connectivity
  – Has a heavy workload in most organizations
  – Only device connected to Internet
  – Providing a single point of contact makes it easier to secure network from hackers
• Functions of a web server
  – Hosts a website
  – Makes it available to the Internet
  – Runs specialized software
    • Apache HTTP Server
    • Microsoft Internet Information Services (IIS)
  – Many businesses use a hosting company instead
Cloud servers
- Not physically located at company office
- Maintained by hosting companies
- Connected to networks via the Internet
- Can be used for any type of server
- Can save money for small businesses
Network Topologies

• Physical or logical arrangement of
  – Computer
  – Transmission media (cable)
  – Other network components

• Physical: Layout of the “real” components of the network
Network Topologies (cont.)

• Logical: Virtual connections among network nodes
  – Determined by protocols instead of physical layout or paths that signals follow
Network Topologies (cont.)

• Network protocols
  – Sets of rules for exchanging information
  – Most common topologies are bus, ring, and star
  – Type of topology affects a network’s performance and scalability
Network Topologies

Bus Topology

• Why a bus topology
  – Bus (linear) topology
    • All computers are connected in sequence
    • Uses a single cable
  – Became legacy technology because of the advantages of star topology
  – Still found where groups of computer-controlled machines are connected
  – Each computer communicates directly with other computers on the network
Network Topologies
Bus Topology (cont.)

A cable break here cuts off Computer #1 and Computer #2 from the rest of the network.
Network Topologies

Bus Topology (cont.)

- Why a bus topology (cont.)
  - Data collisions happen when two computers send data at the same time
  - Causes lost or damaged data
  - Happens frequently in bus networks
  - Access method controls which computer is allowed to use the transmission media at a certain time
  - Taking turns sending data prevents data collisions
Network Topologies
Bus Topology (cont.)

• How data gets from point to point on a bus network
  – Data is broadcast to all devices on the network
  – Data is broken into small segments (packets)
  – Each packet contains the address of computer to which it is being sent
  – Each computer listens for data that has its address
Network Topologies

Bus Topology (cont.)

• How data gets from point to point on a bus network (cont.)
  – Passive topology – when each node does nothing to move data along
  – Terminators
    • Devices that absorb signals so they are not reflected back
    • Found on ends of cable
Network Topologies
Bus Topology (cont.)

• Advantages and disadvantages of bus networks
  – Advantages
    • Simplicity
    • Low cost
  – Disadvantages
    • If there is a break in cable, the network is disrupted
    • Adding a large number of nodes limits performance and causes delays
Network Topologies

Ring Topology

• What a ring topology looks like
  – Configuration resembles a circle
  – Data flows around the circle in one direction
  – Data is passed in special packets (tokens)
  – Once called token-ring topology
Network Topologies
Ring Topology (cont.)

STEP 1: The token travels around the ring until a computer needs to transmit data.

STEP 2: Computer #2 needs to print and grabs the token.

STEP 3: Computer #2 completes the transmission and releases the token.

STEP 4: A cable break stops movement of the token and data transmission.
Network Topologies
Ring Topology (cont.)

• How a token moves data around a ring
  – Token is passed until it is grabbed by a computer that needs to transmit data
  – Computer “holds” token until it is finished transmitting data
  – Only one computer can “hold” the token at a time
  – Token is taken out of circulation until data transmission is complete
Network Topologies
Ring Topology (cont.)

• How a token moves data around a ring (cont.)
  – Token Method
    • A new token is generated, which starts around the ring
    • Used to avoid data collision
    • Active topology: The nodes participate in moving the token
    • Each node is responsible to retransmit the token or data to next mode
    • Large networks use multiple tokens
Network Topologies
Ring Topology (cont.)

- Advantages of a ring topology
  - Provides a fairer allocation of network resources
  - Enables all nodes to have an equal chance to send data
  - Performance is acceptable even with large number of users
Disadvantages of a ring topology

- If one computer fails the entire network can fail.
- Problems in the ring can be hard to find.
- Adding a node causes ring to cease to function while node is being installed.
Network Topologies

Star Topology

• The layout of a star topology
  – Most widely deployed client/server topology
  – Offers the most flexibility for a low price
  – Nodes connect to a central communications device called a switch in a star pattern
  – Switch receives a signal and retransmits to the appropriate node
  – Each node only picks up transmissions addressed to it
Network Topologies
Star Topology (cont.)

• The layout of a star topology (cont.)
  – Active topology because switch retransmits data
  – If switch fails the network no longer functions
  – Relatively easy to replace a switch
Network Topologies

Star Topology (cont.)

A cable break here means Computer #1 cannot communicate with the network. However, all other computers and devices can still communicate with each other.
Network Topologies

Star Topology (cont.)

• How computers on a star network avoid data collisions
  – Most use Ethernet networks
  – Use CSMA/CD (carrier sense multiple access with collision detection)
• Nodes use carrier sense (it “listens”) to verify that no nodes are transmitting data
  – All nodes have same right to transmit data
  – If two devices begin to transmit, the signals will collide
Network Topologies
Star Topology (cont.)

• What happens when signals collide
  – A node detects the collision
  – A jam signal is sent to all nodes alerting them of collision
  – Original nodes stop transmitting
  – After random amount of time the nodes try transmitting again
Network Topologies
Star Topology (cont.)

**STEP 1:** Nodes 1 and 2 transmit data at the same time.

Data collision

**STEP 2:** Node 3 detects a data collision and sends a jam signal.

**STEP 3:** Node 2 retransmits its data after waiting a random interval.
Network Topologies
Star Topology (cont.)

• Advantages of star topology
  – Failure of one computer doesn’t affect rest of network
  – Easy to add nodes
  – Performance remains acceptable even with large number of nodes
  – Centralized communications makes troubleshooting and repairs easier
Network Topologies
Star Topology (cont.)

• Disadvantage of star topology
  – Cost
Network Topologies
Comparing Topologies

- Best topology
  - Star topology is the most common
  - New users being added constantly
  - Installing an additional switch without affecting other users is deciding factor
    - Bus topology is all but extinct
    - Star topology is used in most home networks
    - Ring topology is popular where fair allocation is a major requirement
### Advantages and Disadvantages of Bus, Ring, and Star Topologies

<table>
<thead>
<tr>
<th>TOPOLOGY</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
</table>
| Bus       | - Uses a minimal amount of cable.  
            - Installation is easy, reliable, and inexpensive. | - Breaks in the cable can disable the network.  
            - Large numbers of users decrease performance because of high volumes of data traffic. |
| Ring      | - Allocates access to the network fairly.  
            - Performance remains acceptable even with many users. | - Adding/removing nodes disables the network.  
            - Failure of one node can bring down the network.  
            - Problems in data transmission can be difficult to find. |
| Star      | - Failure of one node doesn’t affect other nodes on the network.  
            - Centralized design simplifies troubleshooting and repairs.  
            - High scalability: Adding computers is easy.  
            - Performance remains acceptable even with many users. | - Requires more cable (and possibly higher installation costs) than a bus or ring topology.  
            - The switch is a single point of failure; if it fails, all computers connected to it are affected. |
Topologies can be combined within a single network

- Topologies are often combined to benefit from the unique advantages of each
- Known as a hybrid topology
Transmission Media

• Transmission media
  – Comprises the physical system that data takes to flow between devices on the network
  – Required or network devices would be unable to communicate
  – Most corporate networks use a combination of wired and wireless media
• Why wired connections are used in business networks
  – Provide higher throughput and better security
  – Desktop computers are still popular choices because of power and speed
  – Permanence of desktop installation lends itself to wired connection
Transmission Media
Wired Transmission Media (cont.)

• Important factors in choosing a cable type
  – Three main cable types
    • Twisted-pair
    • Coaxial
    • Fiber-optic
• Important factors in choosing a cable type (cont.)
  – Six factors need to be considered
    • Maximum run length
    • Bandwidth
    • Bend radius (flexibility)
    • Cable cost
    • Installation cost
    • Interference
Wired Transmission Media (cont.)

- Causes of interference with data signals
  - Electromagnetic interference (EMI)
    - Caused when cable is exposed to strong electromagnetic fields
    - Can distort signals
    - Fluorescent lights, motors, and transformers are most common sources
Transmission Media

Wired Transmission Media (cont.)

• Causes of interference with data signals (cont.)
  – Radio frequency interference (RFI)
    – Broadcast sources located near network
  – Fiber-optic cable is virtually immune to interference
Transmission Media
Twisted-Pair Cable

• Why the wires in twisted-pair cable are twisted
  – Cause the magnetic fields around the wires to intermingle, making them less susceptible
  – Reduce the amount of crosstalk (tendency for signals to interfere with signals next to it)
Transmission Media
Twisted-Pair Cable

• Why the wires in twisted-pair cable are twisted (cont.)
  – Shielded twisted-pair (STP) has a foil shielding
  – Unshielded twisted-pair (UTP) is more susceptible to interference
  – Because of lower cost UTP is most often used
Transmission Media
Twisted-Pair Cable (cont.)

- Twisted pairs of copper wires
- Protective sheath
- Twisted pairs of copper wires
- Protective sheath
- Foil shielding
Coaxial cable in business networks
- Not as popular, but still used when there is heavy electrical interference
Transmission Media
Coaxial Cable (cont.)

• Coaxial cable in business networks (cont.)
  – Four main components of coax cable
    • Core (usually copper) in the center - used for transmitting signal
    • Solid layer of nonconductive insulating material (usually a hard, thick plastic) surrounds the core
    • Layer of braided metal shielding covers the insulation to reduce interference with signals
    • External jacket covers the internal cable components to protect them from damage
What fiber-optic cable looks like

- Three major components
  - Glass (or plastic) fiber (or bundle of fibers) through which data is transmitted
  - Protective layer of glass or plastic wrapped around core to protect it
  - Outer jacket (sheath) made of durable material

- Transmission passes in only one direction, so most cables have at least two fibers (cores)
Transmission Media
Fiber-Optic Cable (cont.)

- Protective sheath
- Glass or plastic cladding
- Optical glass fiber
Transmission Media
Wireless Media Options

- Wireless media options
  - Most businesses use the same Ethernet standards as home networks
  - Wireless access points provide coverage wherever portable devices will be used
  - Example: Conference rooms
Transmission Media
Comparing Transmission Media

• Best medium for business networks
  – Network engineers are responsible for selecting the appropriate topologies and media
    • Topology to be used
    • Length of cable runs
    • Amount of interference
    • Need for wireless connectivity
  – Most use a mix of media types
Network Adapters

• Network adapters
  – Devices that perform specific tasks
  – Enable nodes to communicate on a network
  – Installed inside computers and peripherals
  – Referred to as network interface cards (NICs)
Network Adapters (cont.)

• What network adapters do
  – Generate high-powered signals to enable network transmissions
    • Signals in the computer are low powered
    • Network adapters convert those to higher powered
  – Break the data into packets and transmit and receive data
    • Reconstruct received packets
  – Act as gatekeepers for information flowing to and from the client computer
Network Adapters (cont.)

STEP 1: You request information from the network database.

STEP 2: The NIC breaks the request into packets and sends the packets to the server.

Network interface card (NIC)

STEP 3: The server executes the request, assembles the response into packets, and sends the packets to the client.

STEP 4: The NIC reassembles the response packets and displays information on your screen.

Request packet #1

Request packet #2

Request packet #3

Response packet #1

Response packet #2

Response packet #2

Server
Network Adapters (cont.)

- Different types of network adapters
  - Ethernet is the standard protocol in client/server networks
  - Adapter cards shipped in computers are Ethernet compliant
Network Adapters (cont.)

• Wireless network adapters
  – Any device that connects using wireless access must have a wireless network interface card (wireless NIC)
  – Laptops and other portable devices have a wireless NIC built in
  – Network must have wireless access point (WAP) which gives devices a sending and receiving connection to the network
Network Adapters (cont.)

• Software for network adapters
  – Communications software called device drivers must be installed on all client computers
  – Device drivers enable the network adapter to communicate with the server’s operating system (OS) and computer’s OS
Network Navigation Devices

- Data flows through network in packets
- Data needs help getting to its destination
Network Navigation Devices
MAC Addresses

• How network adapters know where to send data packets
  – Network adapters have a physical address, called a media access control (MAC) address
  • Made up of six two-position characters
  • First three sets indicate the manufacturer
  • Second three sets make up a unique address
Network Navigation Devices
MAC Addresses

• How network adapters know where to send data packets (cont.)
  – Institute of Electrical and Electronics Engineers (IEEE) allocates unique MAC addresses
MAC addresses are not the same as IP addresses

- MAC address is used internally on a network
- Internet Protocol (IP) address is the external address used to communicate with network
- Both addresses are necessary for data to reach its destination
• How data packets are packaged for transmission
  – Packets are not necessarily sent alone
  – A frame is a container for groups of packets which are sent together
  – Network operating system (NOS) assigns the MAC address to the frame
  – NOS keeps track of all devices and their addresses
Network Navigation Devices

MAC Addresses (cont.)

• Delivering the frames to the correct device on the network
  – Small bus network
    • Frames move along the network until the correct client computer pulls the signal off the medium
  – Larger network
    • Not efficient for larger networks
  – Other devices
    • Developed to deliver data efficiently
    • Designed to route signals and exchange data
Other uses of MAC addresses

– Can be used to enhance wireless network security

– A list of authorized MAC addresses can be stored in the router
Network Navigation Devices
Switches and Bridges

• Devices which are used to route signals through a single network
  – Switches send data on a specific route through the network
  – Switch makes decisions using the MAC address to determine where to rebroadcast data
  – Improves network efficiency by ensuring that node only receives data intended for it
Network Navigation Devices
Switches and Bridges (cont.)
• Necessity of a switch in networks
  – All Ethernet networks need a switch
    • Home
    • Business
  – Routers used at home have switches built into them
Network Navigation Devices
Switches and Bridges (cont.)

• Switches are not sufficient for moving data efficiently across networks of all sizes
  – As network grows, performance can decline
  – Network can be broken into segments known as collision domains
  – Bridge is used to send data between collision domains
  – Most home networks only have one segment so a bridge is not necessary
Network Navigation Devices

Routers

• Device a network uses to move data to another network
  – Router is designed to send information between two networks
  – Looks at higher level network addresses
    • IP addresses
    • Not MAC addresses
  – When data address is not on network it sends data to another network or Internet
Network Operating Systems

• Connecting computers together doesn’t create a client/server network
• Network operating system (NOS) is needed
  – Installed on each client and server on network
  – Provides services necessary for communication
  – Provides common rules (protocols) that controls communication
Network Operating Systems (cont.)

• Modern operating systems include NOS as part of their installation
• Large networks require sophisticated NOS software
Network Operating Systems (cont.)

Why a NOS is needed on large networks

- Facilitates communication between software and hardware
- Designed to provide server services
  - Network communications
  - Management of network peripherals
  - Storage
- Client computers must run a small part of NOS
Network Operating Systems (cont.)

• P2P networks need special NOS software
  – Required software is built into Windows, Linux, and Macintosh OS
  – Simple P2P: No need for specialized NOS software
• How the NOS controls network communications
  – Each NOS has proprietary
    • Communications language
    • File management structure
    • Device management structure
  – Sets and controls protocols for all devices
  – Internet uses open protocol (TCP/IP)
  – Modern NOSs support TCP/IP
Using two different NOSs

- Many large corporate networks use several NOSs at the same time
- Different NOSs provide different features
- More useful in certain situations
Network Security for Client/Server Networks

- Sources of security threats all network administrators need to watch for
  - Human errors and mistakes
  - Malicious human activity
  - Natural events and disasters
Network Security for Client/Server Networks

Authentication

• How network administrators ensure that only authorized users access the network
  – Authentication is the process of approving which users can use a network
    • IDs and passwords
    • Biometric devices
    • Possessed objects (an object users carry to identify themselves)
How hackers can use my account to log in to the network

- If ID and password is known you can be impersonated
- If you fail to log out someone else can use your account
How hackers can use my account to log in to the network (cont.)

– User IDs can be easy to figure out
– Brute force attack is the attempt to access an account by repeatedly trying different passwords
– Administrators configure accounts to disable themselves after a set number of invalid login attempts
Access Privileges

• How I can gain access to everything on a network
  – You can’t!
  – Access privileges are granted when your account is set up
  – Indicates which systems you are allowed to use
• How restricting access privileges protects a network
  – Administrator grants access only to systems and software a user needs
  – Centralized nature of network access and ability to restrict access makes client/server more secure than P2P network
• How data theft and destruction occurs
  – Portable devices pose several threats
    • Easily stolen
    • Large memory capacity so many documents can be stored
    • Can introduce viruses
• How network administrators should protect their networks from portable storage devices
  – Educate employees about dangers
  – Create policies regulating use
  – Install security measures such as firewalls
  – Limit and monitor use
• How network administrators should protect their networks from portable storage devices
  – Inform employees that devices are being monitored
  – Deploy monitoring software
Physical Protection Measures

- Physical measures used to protect a network
  - Restrict physical access to sensitive equipment
  - Access card reader reads information from a magnetic strip
    - Card readers are programmed for authorized ID numbers
Network Security for Client/Server Networks
Physical Protection Measures (cont.)
Physical measures used to protect a network (cont.)

- Biometric authentication devices use unique characteristic of human biology to identify users
- Fingerprints (palm prints), retina scanner
• Problems with biometric devices
  – Don’t always function as intended
    • Fooled by pictures or videos of authorized user
    • Fooled by clay fingers or other imitations
  – Future fingerprint readers will use algorithms to detect moisture or electrical current
  – Future retinal readers might check for blinks or whether pupils contract
• Internet connections on client/server networks are vulnerable to hackers
  – Any company’s network connected to Internet can attract hackers
  – Any well-defended network includes a firewall
  – Firewalls can be software or hardware based
  – Routers often equipped to act as hardware firewalls
How a firewall on a client/server network works compared to the personal firewall installed on a home network

- Works on same basic principles
- Contains a few extra security options
- Packet screening has an external screening router examine incoming data packets
• How a firewall on a client/server network works compared to the personal firewall installed on a home network (cont.)
  – Unauthorized or suspect packets are discarded
  – Internal screening router detects Trojan horse programs
Network Security for Client/Server Networks
Firewalls (cont.)

• Other security measures the firewall on a client/server network uses
  – Bastion host: A heavily secured server on a perimeter network
  • Between secure internal network and firewall
    – Internal network is still safe if hacker breaches bastion host
    – Gives network administrators time to detect and thwart hackers’ attacks
Network Security for Client/Server Networks

Firewalls (cont.)

- How bastion hosts help protect systems from hackers
  - Honey pot
    - Computer set up to attract unauthorized users
    - Appears to be a key part of network
    - Pretends to contain something of great value
• How bastion hosts help protect systems from hackers
  – Proxy server: Acts as a go-between connecting internal computers with external network
• All requests goes through proxy server
Chapter 12 Summary Questions

1. What are the advantages of a Business network?
2. How does a client/server network differ from a peer-to-peer network?
3. What are the different classifications of client/server networks?
4. What components are needed to construct a client/server network?
Chapter 12 Summary Questions

5. What do the various types of servers do?
6. What are the various network topologies, and why is network topology important in planning a network?
7. What types of transmission media are used in client/server networks?
8. How do network adapters enable computers to participate in a client/server network?
9. What devices assist in moving data around a client/server network?
10. What software needs to run on computers attached to a client/server network, and how does this software control network communications?
11. What measures are employed to keep large networks secure?