*Technology in Action*

Chapter 7

networking and security:   
connecting computers and keeping them safe   
from hackers and viruses

# CHAPTER REVIEW

Buzz Words/Word Bank

|  |  |  |
| --- | --- | --- |
| antivirus software | identity theft | router |
| Cat 5E | logical port(s) | throughput |
| cybercriminal(s) | network adapter(s) | virus |
| Distributed Denial of Service | network interface card(s) | wired Ethernet |
| firewall | peer-to-peer (P2P) | wireless Ethernet |
| hacker(s) | phone cable | zombie(s) |

**Instructions:** Fill in the blanks using the words from the Word Bank above.

Cathi needed to network three computers for herself and her roommates (Sharon and Emily). She decided that a(n) (1) **peer-to-peer** network was the right type to install in their apartment because that was the most common type of home network. Because none of them were gamers or transferred large files, they didn’t need high (2) **throughput**. Still, they decided to use the fastest type of home network, a(n) (3) **wireless Ethernet** network, because it is reliable and easy to install. To connect the computers, they needed to buy (4) **CAT 5E** cable. Because Sharon already had high-speed Internet access through the cable TV company, she needed to buy a(n) (5) **router** for the network to ensure all users could share the connection. Fortunately, all their computers already had (6) **network interface card(s)** installed, making it easy to connect the computers to the network.

Cathi’s roommate Emily was skeptical of being hooked up to the Internet because she had been the victim of (7) **identity theft**, which destroyed her credit rating. A(n) (8) **cybercriminal** had obtained her credit card information by posing as an employee of her bank. Cathi assured Emily that the router could be configured as a(n) (9) **firewall** to repel malicious (10) **hackers**. Turning off the unused (11) **logical ports** would repel most attacks on their home network. With this protection, it was unlikely that a hacker would turn their PCs into (12) **zombies** to launch (13) **Distributed Denial of Service** attacks. But after the scare with the Melissa (14) **virus**, Cathi was careful to warn the others not to open files from untrusted sources. She also made sure they all installed (15) **antivirus software** on their PCs to protect them from viruses.

**Self-Test**

**Instructions:** Answer the multiple choice and true/false questions below for more practice with key terms and concepts from this chapter.

**MULTIPLE CHOICE**

1. Which of the following is NOT a benefit of installing a home network?
   1. file sharing
   2. peripheral sharing
   3. bandwidth sharing
   4. Internet connection sharing

ANSWER: C

1. Which of the following is NOT a reason why client/server networks are generally not installed in homes?
   1. Servers are too difficult for most home users to set up.
   2. Client/server networks don’t have as many security features as home networks.
   3. Client/server networks provide more security than is needed in a home network.
   4. Client/server networks are more expensive than peer-to-peer networks.

ANSWER: B

1. *All* networks contain the following elements except:
   1. transmission media.
   2. network adapters.
   3. network software.
   4. servers

ANSWER: D

1. Because of their complexity, Ethernet networks require network navigation devices to move data from node to node on the network. An example of such a device is a:
   1. switch.
   2. packet mover.
   3. Cat 5E.
   4. UPS.

ANSWER: A

1. Wireless networks are popular because:
   1. you don’t need wires to install them.
   2. they are much less complicated to set up than wired Ethernet networks.
   3. they cost about two thirds less then wired networks.
   4. All of the above

ANSWER: A

1. Power-line and phoneline networks are no longer very popular mainly because:
   1. they are more expensive than Ethernet networks.
   2. they can’t provide as much throughput as Ethernet networks.
   3. Both A and B
   4. None of the above

ANSWER: C

1. When hackers use computers they have gained control over to launch an attack against a Web site that prevents legitimate users from accessing the site, this is called a:
   1. Zombie Denial of Service Attack.
   2. Worm Virus Attack.
   3. Trojan Horse Attack.
   4. Distributed Denial of Service Attack.

ANSWER: D

1. Which of the following is NOT a benefit of firewalls?
   1. They make it harder for a hacker to locate specific computers on a network.
   2. They repeatedly change the IP address of the router.
   3. They close off unused logical ports.
   4. They filter out unwanted packets.

ANSWER: B

1. Wireless Ethernet networks are attractive to hackers because:
   1. they are easier to penetrate than wired Ethernet networks because the 802.11 protocol has weak security rules.
   2. you can’t install a firewall on a wireless Ethernet network.
   3. the signals from the network can travel beyond the walls of your home.
   4. they have greater bandwidth than wired networks, making it easier for hackers to conceal their activities.

ANSWER: C

1. Viruses that are often hidden in Microsoft Office documents are called:
   1. worms.
   2. stealth viruses.
   3. logic bombs.
   4. macro viruses.

ANSWER: D

**TRUE/FALSE**

**False** 1. Wireless Ethernet networks provide the highest possible throughput for home networks.

**False** 2. All home networks require each computer on the network to be equipped with its own router.

**True** 3. Installing a firewall on your network will stop most hackers from obtaining access to your network through your Internet connection.

**False** 4. Never downloading files from the Internet will ensure your computer is always safe from viruses.

**True** 5. Wireless Ethernet networks are subject to interference from cordless phones and large metal objects.

**Critical Thinking Questions**

**1. Home Networking: A Profession?**

Many people will be installing computer networks in their homes over the next five years.

1. Would starting a home networking installation business be a good entry-level job for a college graduate? Could it be a good part-time job for a college student?
2. Assuming the home networking business failed, what other careers would the technicians be prepared to assume?

*Most students would be likely to agree that this is a good potential home-based business to start. An alternative would be to assist home clients with installing, configuring, and testing antivirus and firewall software. If the home networking business failed, technicians could find jobs as network support personnel in small- to medium-sized companies.*

**2. Upgrading Your Wireless**

You have just finished purchasing and installing a new wireless network in your home. A new wireless standard of networking will be launched next month that is 10 times as fast as the wireless network you installed.

1. What types of applications would you need to be using heavily to make it worth upgrading to the new standard?
2. Did you set up your wireless network securely so that your next-door neighbor can’t tap into it and save himself the cost of purchasing Internet access? Is tapping into a neighbor’s wireless connection that is not secure ethical?

*If the student is doing quite a lot of uploading/downloading of files, or playing games over the Internet, it could be worthwhile upgrading to a new standard of wireless technology. Unfortunately, it is very possible for neighbors to poach bandwidth. The ethics of such a practice seems subject to wide interpretation by today’s students. Be prepared for a lively discussion!*

**3. Ethical Hacking?**

Hackers and virus authors cause millions of dollars worth of damage to PCs and networks annually. But hacking is a very controversial subject. Many hackers believe they are actually working for the “good of the people” or “exercising their freedom” when they engage in hacking activities. However, in most jurisdictions in the United States, hacking is punishable by stiff fines and jail terms.

1. Hackers often argue that hacking is for the good of all people because it points out flaws in computer systems. Do you agree with this? Why or why not?
2. What should the punishment be for convicted hackers and why?
3. Who should be held accountable at a corporation whose network security is breached by a hacker?

*Many students would agree that hackers are antisocial and violate individuals’ right to privacy. However, some students tend to side with the hackers thinking they are “cool” individuals. Be sure to stress that hacking is illegal in almost every country in the world, including the United States. Point out that a system should only be “tested” by a hacker with the blessing of the computer/network owner.*

**4. Keeping Networks Safe from Cyberterrorists**

Many of us rely on networks every day, often without realizing it. Whether using the Internet, ordering a book from Amazon.com, or accessing your college e-mail from home, you are relying on networks to relay information. But what if terrorists destroyed key components of the Internet or other networks on which we depend?

1. What economic problems would result from DDoS attacks launched by terrorists on major e-commerce sites?
2. Research precautions that the U.S. military and intelligence agencies (FBI, CIA) are taking to ensure that networks involving national defense remain secure from terrorist attacks. What else should they do?

*The risks from terrorist attacks are significant. All responsible industries as well as the U.S. government should have significant computer network security, as well as a sound backup/recovery plan in place.*

**5. Protection for Your Computer?**

Do you have a firewall or antivirus software installed on your home computer? If not, why not? Have you ever been a victim of a hacker or a virus?

*Almost all students will have a disaster story about how they or someone they know became a victim of this type of activity. More students are likely to have antivirus software than a firewall. The question is whether they are updating this software on a regular basis and scanning their system on a set schedule.*

**Team Time**

**Creating a Wireless Campus**

*This exercise gives students the opportunity to explore various Wi-Fi problems and many students will take this exercise to very complex lengths as wireless connectivity seems to be very interesting to the majority of students. The following rubric may be useful for grading purposes.*

| **Rubric** | **Beginning**  **1 point** | **Developing**  **2 points** | | **Proficient**  **3 points** | | **Exemplary**  **4 points** | **Score** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Individual Effort** | There was very little effort or understanding of the topic shown. | There was evidence of effort but it lacked in preparation and understanding. | | Clear learning on the topic has occurred. | | A sound understanding of the topic was exhibited with enthusiasm and creativity. |  |
| **Team Effort** | Team members did not function as a group when given the opportunity. There was only individual work with no evidence of collaboration. | Team members had some major problems working as a group. There was little collaboration and teamwork evident. | | The team members mostly worked well together, with few problems. There could have been improvement in the level of teamwork that was utilized. | | The team worked as a cohesive unit. There was mature collaboration, compromise, and discussion evident at all times. |  |
| **Final Product** | The final presentation had major factual, grammatical, spelling, and formatting errors. It seemed rushed and incomplete. | The final presentation had factual, grammatical, spelling, or formatting errors but was complete. | | The final presentation was a carefully developed product with few factual, grammatical, spelling, or formatting errors. | | The presentation was developed with care and creativity making it interesting, polished, and error-free. |  |
| **Instructor Feedback** | Little or no attempt was made to receive or incorporate feedback from the instructor. | Feedback was received, but none of the suggestions were incorporated into the presentation. | | Feedback was received and some suggestions were incorporated into the presentation. | | Feedback was received and the suggestions were incorporated into the presentation. |  |
| **Evaluation** | 0 points  No assessments were completed and handed in to the instructor. | | 1 point  One assessment was completed and handed in to the instructor. | | 2 points  All assessments were completed and handed in to the instructor. | |  |

**Multimedia**

In addition to the review materials presented here, you’ll find additional materials featured with the book’s multimedia, including the *Technology in Action* Student Resource CD and the Companion Web site ([www.prenhall.com/techinaction](http://www.prenhall.com/techinaction)), which will help reinforce student understanding of the chapter content. These materials include the following:

**ACTIVE HELPDESK**

These exercises are designed to provide the student with an interactive experience that will help them to extend their knowledge of topics in this chapter. The student plays the “role” of a Helpdesk analyst and provides answers to *commonly* asked questions in a rich, simulated online experience. Helpdesk calls can be found on the Train and Assess IT Web site, through your online course, or on the Student CD. After successfully completing the Helpdesk call, students will be able to access the Helpdesk Cheat Sheet, which summarizes the key points in each call.

The Helpdesk calls related to this chapter are:

* Understanding Networking
* Understanding Firewalls
* Avoiding Computer Viruses

***Understanding Networking******Helpdesk Cheat Sheet***

***A. Networks***

*A* ***computer network*** *is two or more computers connected together via software and hardware so that they can communicate. Devices connected to a network are called* ***nodes****. Networks allow users to share peripherals such as printers, to transfer files from one computer to another without using external storage media, and to share broadband Internet connections.*

***B. Types of Networks***

***1. Peer-to-Peer (P2P):*** *Each node on the network can communicate directly with every other node. No separate device is needed to control the network. The most common type of home network.*

***2. Client/Server:*** *Contains clients and servers. A* ***client*** *is a computer that requests services from the server computer. A* ***server*** *is a computer that provides resources to client computers and provides central control of the network. Used for networks with over 10 nodes.*

***C. Wireless Networks***

*A* ***wireless network*** *uses radio waves instead of wires****.*** *Wireless networks in the United States are based on the* ***802.11 standard****, also known as* ***Wi-Fi****. For home networking, two main standards exist:* ***802.11b*** *and* ***802.11g****.*

***D. Ethernet Networks***

***Ethernet networks*** *use the Ethernet protocol as the means by which the nodes communicate. Ethernet networks are fast and reliable and are the most popular choice for wired home networks.*

***E. Network Adapters***

***Network adapters*** *are devices that enable the nodes on a network to access the network and communicate with each other. Some network adapters are external devices that plug into a USB port. Others, called* ***network interface cards (NICs)****, are installed inside computers and peripherals. Wireless networks require special* ***wireless network adapters****.*

***F. Transmission Media***

*A* ***transmission medium*** *establishes a communications channel between nodes on a network.* ***Data transfer rate*** *is the maximum speed at which data can be transmitted between nodes on a network.. Wired networks use different kinds of cable to connect nodes:*

*1.* ***Twisted-Pair Cable:*** *Made up of copper wires twisted around each other and surrounded by plastic. There are two types:* ***unshielded twisted pair (UTP)*** *and* ***shielded******twisted pair (STP).*** *The most popular option for Ethernet networks is UTP.*

*2.* ***Coaxial Cable****: Consists of a copper wire surrounded by plastic. The cable running from a TV to a cable box is coaxial cable.*

***3. Fiber-Optic Cable:*** *Made up of plastic or glass fibers that transmit data very fast. Because of its cost, it is used mostly on client/server networks.*

***G. Network Navigation Devices***

*Data is sent over transmission media in bundles called* ***packets****.* ***Network navigation devices*** *are attached to the network to enable the transmission of data.* ***Routers*** *are devices that route packets of data between two or more networks. If a home network is connected to the Internet, it needs a router to send data between the network and the Internet.*

***Understanding Firewalls Helpdesk Cheat Sheet***

***Firewalls***

***1. Everyone Needs a Firewall:*** *All users, regardless of whether they have a broadband or dial-up Internet connection, need a firewall if they connect to the Internet.*

***2. What Risks Firewalls Protect Against:*** *Even if you don’t store proprietary files on your home computers, hackers can still use it for other illegal activities, such as to commit identity theft, to launch a Trojan horse, or to launch a denial-of-service attack.*

***3. How Firewalls Work:*** *A firewall protects a computer by screening data coming into the computer’s logical ports to see whether it is from a trusted source. Logical ports allow a computer to organize requests for information from other networks or computers. Unless you take precautions to restrict access to your logical ports, hackers may be able to access your computer through them.*

***4. Types of Firewalls:*** *Firewalls can be either software programs or hardware devices, both of which are equally effective.**Personal firewalls are software programs or hardware devices specifically designed to keep home computers safe from hackers.*

***5. Buying Firewalls:*** *You can get free firewall software from* [*www.download.com*](http://www.download.com/) *or you can buy firewall software or hardware devices at computer retail stores.*

**6. Installing and Testing Firewalls:** Although some people prefer to have a professional install and test their firewall, even home users can install and test a firewall by following the instructions provided in the user manual. Unfortunately, not all firewalls come with software that allows you to test whether the firewall is working correctly. The best solution is to test the firewall with a testing agent such as ShieldsUp!

***Avoiding Computer Viruses******Helpdesk Cheat Sheet***

***1. Virus Symptoms.*** *A computer virus is a computer program that attaches itself to another computer program and attempts to spread itself to other computers when files are exchanged. There are several symptoms of computer viruses, including program icons or files disappearing, browser settings changing, and odd messages or images being displayed on the screen.*

***2. Types of Viruses.*** *There are many types of viruses.*

***A. Boot-sector viruses:*** *These viruses replicate themselves into the hard drive’s master boot record. You get boot sector viruses by booting up your computer with an infected disk in the disk drive.*

***B. Macro viruses:*** *These viruses are attached to documents (usually Word or Excel) that contain macros. If you enable macros in an infected document, the virus will be triggered.*

***C. E-mail viruses:*** *You can get some viruses by downloading or running a file attached to an e-mail message. Other e-mail viruses use your e-mail address book to spread on their own.*

***D. Logic bombs:*** *These viruses execute when a certain set of conditions is met and are spread when infected files are passed from user to user.*

***E. Scripts:*** *Some viruses are hidden on Web sites in the form of scripts.*

***F. Trojan horses:*** *Once executed, Trojan horses perform their malicious duties in the background, often invisible to the user.*

***G. Worms:*** *Slightly different from viruses, worms travel between systems through network connections.*

***3. Antivirus Software.*** *The best defense against viruses is to install antivirus software, which scans files when they’re opened or executed and detects virus signatures or suspicious activities and stops them.*

***A. Types of software:*** *Popular antivirus programs include McAfee Virusscan, Norton AntiVirus, and PC-cillin.*

***B. Auto-enabling:*** *You can set your antivirus software to run checks automatically when you aren’t using your system.*

***4. Other Defensive Tactics.*** *To minimize the risk of your computer being attacked by a new virus your software can’t detect, you need to keep both your antivirus software and your system software up to date.*