

CEA-CompTIA DHTI+ Certification

Instructor's Edition

THOMSON
—★—™
COURSE TECHNOLOGY

Australia • Canada • Mexico • Singapore
Spain • United Kingdom • United States

NOT FOR PRINTING OR INSTRUCTIONAL USE

CEA-CompTIA DHTI+ Certification

VP and GM, Training Group: Michael Springer
Series Product Managers: Charles G. Blum and Adam A. Wilcox
Developmental Editor: Gail Sandler
Copyeditor: Cathy Albano
Keytester: Gail Sandler
Series Designer: Adam A. Wilcox
Cover Designer: Abby Scholz

COPYRIGHT © 2007 Course Technology, a division of Thomson Learning. Thomson Learning is a trademark used herein under license.

ALL RIGHTS RESERVED. No part of this work may be reproduced, transcribed, or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution, or information storage and retrieval systems—without the prior written permission of the publisher.

For more information contact:

Course Technology
25 Thomson Place
Boston, MA 02210

Or find us on the Web at: www.course.com

For permission to use material from this text or product, submit a request online at: www.thomsonrights.com

Any additional questions about permissions can be submitted by e-mail to: thomsonrights@thomson.com

Trademarks

Course ILT is a trademark of Course Technology.

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Disclaimer

Course Technology reserves the right to revise this publication and make changes from time to time in its content without notice.

The logo of the CompTIA Authorized Quality Curriculum (CAQC) program and the status of this or other training material as “Authorized” under the CompTIA Authorized Quality Curriculum program signifies that, in CompTIA’s opinion, such training material covers the content of CompTIA’s related certification exam.

The contents of this training material were created for the CEA-CompTIA DHTI+ exam covering CEA-CompTIA certification objectives that were current as of April 2007.

CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such “Authorized” or other training material in order to prepare for any CompTIA certification exam.

ISBN-10: 1-4260-9140-0

ISBN-13: 978-1-4260-9140-7

Printed in the United States of America

1 2 3 4 5 GLOB 06 05 04 03

NOT FOR PRINTING OR INSTRUCTIONAL USE

Contents

Introduction	iii
Topic A: About the manual.....	iv
Topic B: Setting student expectations	ix
Topic C: Classroom setup.....	xv
Topic D: Support.....	xviii
Introduction to DHTI	1-1
Topic A: Digital home technology integration	1-2
Topic B: Basic components of DHTI systems.....	1-14
Topic C: Designing and installing DHTI systems	1-23
Topic D: After the installation of DHTI systems.....	1-26
Unit summary: Introduction to DHTI	1-30
Computer networking	2-1
Topic A: Networking configuration.....	2-2
Topic B: Resource sharing.....	2-28
Topic C: Internet connectivity	2-34
Topic D: Network protection	2-52
Unit summary: Computer networking.....	2-87
Audio/video system concepts	3-1
Topic A: Residential home theater systems	3-2
Topic B: Content management systems.....	3-27
Topic C: Implementing multi-room audio/video systems	3-35
Unit summary: Audio/video system concepts.....	3-44
Telephony and VoIP	4-1
Topic A: Plain Old Telephone Systems	4-2
Topic B: Voice over IP	4-13
Topic C: Telephone systems.....	4-24
Unit summary: Telephony and VoIP.....	4-32
Security and surveillance systems	5-1
Topic A: Security and surveillance system components.....	5-2
Topic B: Security system installation	5-13
Topic C: Security and surveillance cameras.....	5-29
Topic D: Security system peripherals and accessories	5-38
Unit summary: Security and surveillance systems.....	5-48
Home control and management	6-1
Topic A: Control systems integration	6-2
Topic B: HVAC control.....	6-16
Topic C: Lighting control	6-26
Topic D: Power protection.....	6-38
Unit summary: Home control and management.....	6-43
Troubleshooting DHTI systems	7-1
Topic A: DHTI troubleshooting and diagnostics	7-2

Topic B: Troubleshooting wireless systems.....	7-13
Topic C: Troubleshooting integrated subsystems	7-19
Unit summary: Troubleshooting DHTI systems.....	7-37
Certification exam objectives map	A-1
Topic A: Comprehensive exam objectives.....	A-2
CEA-CompTIA DHTI+ acronyms	B-1
Topic A: Acronyms list	B-2
Course summary	S-1
Topic A: Course summary.....	S-2
Topic B: Continued learning after class.....	S-4
Glossary	G-1
Index	I-1

Introduction

After reading this introduction, you will know how to:

- A** Use Course Technology ILT manuals in general.
- B** Use prerequisites, a target student description, course objectives, and a skills inventory to properly set students' expectations for the course.
- C** Set up a classroom to teach this course.
- D** Get support for setting up and teaching this course.

Topic A: About the manual

Course Technology ILT philosophy

Our goal at Course Technology is to make you, the instructor, as successful as possible. To that end, our manuals facilitate students' learning by providing structured interaction with the software itself. While we provide text to help you explain difficult concepts, the hands-on activities are the focus of our courses. Leading the students through these activities will teach the skills and concepts effectively.

We believe strongly in the instructor-led classroom. For many students, having a thinking, feeling instructor in front of them will always be the most comfortable way to learn. Because the students' focus should be on you, our manuals are designed and written to facilitate your interaction with the students, and not to call attention to manuals themselves.

We believe in the basic approach of setting expectations, then teaching, and providing summary and review afterwards. For this reason, lessons begin with objectives and end with summaries. We also provide overall course objectives and a course summary to provide both an introduction to and closure on the entire course.

Our goal is your success. We encourage your feedback in helping us to continually improve our manuals to meet your needs.

Manual components

The manuals contain these major components:

- Table of contents
- Introduction
- Units
- Appendices
- Course summary
- Glossary
- Index

Each element is described below.

Table of contents

The table of contents acts as a learning roadmap for you and the students.

Introduction

The introduction contains information about our training philosophy and our manual components, features, and conventions. It contains target student, prerequisite, objective, and setup information for the specific course. Finally, the introduction contains support information.

Units

Units are the largest structural component of the actual course content. A unit begins with a title page that lists objectives for each major subdivision, or topic, within the unit. Within each topic, conceptual and explanatory information alternates with hands-on activities. Units conclude with a summary comprising one paragraph for each topic, and an independent practice activity that gives students an opportunity to practice the skills they've learned.

The conceptual information takes the form of text paragraphs, exhibits, lists, and tables. The activities are structured in two columns, one telling students what to do, the other providing explanations, descriptions, and graphics. Throughout a unit, instructor notes are found in the left margin.

Appendices

This course has two appendices:

- Appendix A lists all CEA-CompTIA DHTI+ exam objectives, along with references to corresponding coverage in this course.
- Appendix B provides a list of acronyms that appear on the CEA-CompTIA DHTI+ exam.

Course summary

This section provides a text summary of the entire course. It is useful for providing closure at the end of the course. The course summary also indicates the next course in this series, if there is one, and lists additional resources students might find useful as they continue to learn about the software.

Glossary

The glossary provides definitions for all of the key terms used in this course.






Index

The index at the end of this manual makes it easy for you and your students to find information about a particular software component, feature, or concept.

Manual conventions

We've tried to keep the number of elements and the types of formatting to a minimum in the manuals. We think this aids in clarity and makes the manuals more classically elegant looking. But there are some conventions and icons you should know about.

Instructor note/icon

Convention	Description
<i>Italic text</i>	In conceptual text, indicates a new term or feature.
Bold text	In unit summaries, indicates a key term or concept. In an independent practice activity, indicates an explicit item that you select, choose, or type.
Code font	Indicates code or syntax.
Longer strings of code will look like this.	In the hands-on activities, any code that's too long to fit on a single line is divided into segments by one or more continuation characters (►). This code should be entered as a continuous string of text.
<i>Instructor notes.</i>	In the left margin, provide tips, hints, and warnings for the instructor.
Select bold item	In the left column of hands-on activities, bold sans-serif text indicates an explicit item that you select, choose, or type.
Keycaps like 	Indicate a key on the keyboard you must press.
 <i>Warning icon.</i>	Warnings prepare instructors for potential classroom management problems.
 <i>Tip icon.</i>	Tips give extra information the instructor can share with students.
 <i>Setup icon.</i>	Setup notes provide a realistic business context for instructors to share with students, or indicate additional setup steps required for the current activity.
 <i>Projector icon.</i>	Projector notes indicate that there is a PowerPoint slide for the adjacent content.

Hands-on activities

The hands-on activities are the most important parts of our manuals. They are divided into two primary columns. The “Here’s how” column gives short directions to the students. The “Here’s why” column provides explanations, graphics, and clarifications. To the left, instructor notes provide tips, warnings, setups, and other information for the instructor only. Here’s a sample:

Do it!

Take the time to make sure your students understand this worksheet. We'll be here a while.

A-1: Creating a commission formula

Here's how	Here's why
1 Open Sales	This is an oversimplified sales compensation worksheet. It shows sales totals, commissions, and incentives for five sales reps.
2 Observe the contents of cell F4	<div> <div>F4</div> <div>▼</div> <div>=</div> <div>E4*C_Rate</div> </div> <p>The commission rate formulas use the name “C_Rate” instead of a value for the commission rate.</p>

For these activities, we have provided a collection of data files designed to help students learn each skill in a real-world business context. As students work through the activities, they will modify and update these files. Of course, they might make a mistake and, therefore, want to re-key the activity starting from scratch. To make it easy to start over, students will rename each data file at the end of the first activity in which the file is modified. Our convention for renaming files is to add the word “My” to the beginning of the file name. In the above activity, for example, students are using a file called “Sales” for the first time. At the end of this activity, they would save the file as “My sales,” thus leaving the “Sales” file unchanged. If students make mistakes, they can start over using the original “Sales” file.

In some activities, however, it may not be practical to rename the data file. Such exceptions are indicated with an instructor note. If students want to retry one of these activities, you will need to provide a fresh copy of the original data file.

PowerPoint presentations

Each unit in this course has an accompanying PowerPoint presentation. These slide shows are designed to support your classroom instruction while providing students with a visual focus. Each one begins with a list of unit objectives and ends with a unit summary slide. We strongly recommend that you run these presentations from the instructor's station as you teach this course. A copy of PowerPoint Viewer is included, so it is not necessary to have PowerPoint installed on your computer.

The Course ILT PowerPoint add-in

The CD also contains a PowerPoint add-in that enables you to do two things:

- Create slide notes for the class
- Display a control panel for the Flash movies embedded in the presentations

To load the PowerPoint add-in:

- 1 Copy the Course_ILT.ppa file to a convenient location on your hard drive.
- 2 Start PowerPoint.
- 3 Choose Tools, Macro, Security to open the Security dialog box. On the Security Level tab, select Medium (if necessary), and then click OK.
- 4 Choose Tools, Add-Ins to open the Add-Ins dialog box. Then, click Add New.
- 5 Browse to and select the Course_ILT.ppa file, and then click OK. A message box will appear, warning you that macros can contain viruses.
- 6 Click Enable Macros. The Course_ILT add-in should now appear in the Available Add-Ins list (in the Add-Ins dialog box). The "x" in front of Course_ILT indicates that the add-in is loaded.
- 7 Click Close to close the Add-Ins dialog box.

After you complete this procedure, a new toolbar will be available at the top of the PowerPoint window. This toolbar contains a single button labeled "Create SlideNotes." Click this button to generate slide notes files in both text (.txt) and Excel (.xls) format. By default, these files will be saved to the folder that contains the presentation. If the PowerPoint file is on a CD-ROM or in some other location to which the SlideNotes files cannot be saved, you will be prompted to save the presentation to your hard drive and try again.

When you run a presentation and come to a slide that contains a Flash movie, you will see a small control panel in the lower-left corner of the screen. You can use this panel to start, stop, and rewind the movie, or to play it again.

Topic B: Setting student expectations

Properly setting students' expectations is essential to your success. This topic will help you do that by providing:

- Prerequisites for this course
- A description of the target student at whom the course is aimed
- A list of the objectives for the course
- A skills assessment for the course

Course prerequisites

Students taking this course should be familiar with personal computers and the use of a keyboard and a mouse. Furthermore, this course assumes that students have earned the following certifications or have equivalent experience:

- CompTIA A+ certification
- CompTIA Network+ certification

Target student

This course is for students who are preparing for the CEA-CompTIA DHTI+ exam (see below). They should already have the baseline skills and requisite knowledge for working with PC hardware, hand and tool skills, safety precautions, basic electrical awareness, local regulations and building codes.

How to become CompTIA certified

In order to achieve CEA-CompTIA DHTI+ certification, a student must register for and pass the the CEA-CompTIA DHTI+ certification exam (HT0-201). In order to become CompTIA certified, students must:

- 1 Select a certification exam provider. For more information, students should visit: <http://certification.comptia.org/resources/registration.aspx>
- 2 Register for and schedule a time to take the CompTIA certification exam(s) at a convenient location.
- 3 Read and sign the Candidate Agreement, which is presented at the time of the exam. The complete text of the Candidate Agreement can be found at: http://certification.comptia.org/resources/candidate_agreement.aspx
- 4 Take and pass the CompTIA certification exam(s).

For more information about CompTIA's certifications, such as its industry acceptance, benefits, or program news, students should visit: <http://certification.comptia.org>

CompTIA is a not-for-profit information technology (IT) trade association. CompTIA's certifications are designed by subject matter experts from across the IT industry. Each CompTIA certification is vendor-neutral, covers multiple technologies, and requires demonstration of skills and knowledge widely sought after by the IT industry.

To contact CompTIA with any questions or comments, please call (630) 678-8300 or e-mail questions@comptia.org.

Course objectives

You should share these overall course objectives with your students at the beginning of the day. This will give the students an idea about what to expect, and will also help you identify students who might be misplaced. Students are considered misplaced when they lack the prerequisite knowledge or when they already know most of the subject matter to be covered.

Note: In addition to the general objectives listed below, specific CEA-CompTIA DHTI+ exam objectives are listed at the beginning of each topic. For a complete mapping of exam objectives to course content, see Appendix A.

After completing this course, students will know how to:

- Identify what HTI is, its components, and how to design and install HTI systems.
- Design and configure home networks.
- Install and configure audio and video components.
- Install and configure telecommunications systems.
- Install and set up security systems.
- Install and configure control systems.
- Troubleshoot home technology subsystems.

Skills inventory

Use the following form to gauge students' skill level entering the class (students have copies in the introductions of their student manuals). For each skill listed, have students rate their familiarity from 1 to 5, with 5 being the most familiar. Emphasize that this is not a test. Rather, it is intended to provide students with an idea of where they're starting from at the beginning of class. If a student is wholly unfamiliar with all the skills, he or she might not be ready for the class. A student who seems to understand all of the skills, on the other hand, might need to move on to the next course in the series.

Skill	1	2	3	4	5
Identifying features of Home Technology Integration					
Identifying functions of DHTI systems					
Identifying benefits of DHTI systems					
Identifying components of DHTI systems					
Researching DHTI products on the Internet					
Finding components for a control system on the Internet					
Designing a whole-house lighting control system					
Determining the availability and cost of Internet service in your area					
Delivering manuals and documentation to the end user					
Verifying the installation					
Discussing network models					
Installing a wireless network adapter					
Discussing when to use hard-wired vs. wireless networks					
Identifying characteristics of wired cable types					
Viewing installed network protocols					
Configuring an IP address and subnet mask					
Configuring additional TCP/IP properties					
Joining a Windows workgroup					
Viewing network resources					
Sharing a folder					
Connecting to a shared folder					
Sharing a printer					

Skill	1	2	3	4	5
Connecting to a shared printer					
Identifying Internet technologies					
Selecting a connection technology					
Discussing network media					
Configuring Windows Firewall					
Installing protection software					
Blocking pop-ups					
Installing a spyware checker					
Controlling cookies					
Setting security zones					
Identifying the technology used to implement WLANs					
Configuring a wireless access point					
Configuring a wireless client					
Defining acoustical terms					
Identifying multi-channel surround options					
Identifying display types					
Defining video terms					
Planning installation and configuration of a home theater system					
Identifying content sources					
Discussing media storage types					
Considering digital rights management					
Setting up audio system components					
Setting up video system components					
Configuring audio/video system components					
Testing audio/video system components					
Setting up a multi-room wireless A/V system					
Defining POTS features					

Skill	1	2	3	4	5
Setting up and configuring POTS access					
Identifying common POTS issues					
Defining VoIP features					
Setting up and configuring VoIP access					
Testing the quality of VoIP on your PC					
Connecting telephone extensions and lines to a PBX					
Identifying telephone system features					
Implementing a telephone system					
Identifying security peripherals and accessories					
Identifying security monitoring formats					
Examining security infrastructure types					
Discussing wireless security system installation					
Identifying access control devices and protocols					
Installing and configuring a security panel					
Discussing camera types and specifications					
Identifying camera applications					
Installing entry components					
Installing interior components					
Installing and configuring cameras					
Installing environmental sensors					
Testing the security and surveillance system					
Installing a PC-based control system					
Using a PC as a control system user interface					
Examining control system communication protocols					
Discussing HVAC control					
Programming thermostats					
Programming lights to turn on when motion is detected					

Skill	1	2	3	4	5
Installing lighting control devices					
Identifying whole house protection options					
Installing power point protection					
Measuring electrical values					
Using cable testing equipment					
Troubleshooting problems					
Troubleshooting wireless interference problems					
Troubleshooting network subsystems					
Troubleshooting audio/video subsystems					
Troubleshooting telephony subsystems					
Troubleshooting security and surveillance subsystems					
Troubleshooting automated lighting systems					

Topic C: Classroom setup

All our courses assume that each student has a personal computer to use during the class. Our hands-on approach to learning requires they do. This topic gives information on how to set up the classroom to teach this course. It includes minimum requirements for the students' personal computers, setup information for the first time you teach the class, and setup information for each time that you teach after the first time you set up the classroom.

Student computer requirements

Each student's personal computer should have:

- A keyboard and a mouse
- A 300 MHz or higher processor
- 256 MB RAM
- 1 GB hard drive
- CD-RW drive
- A monitor (SVGA)
- A network card installed
- Internet access
- A sound card
- A microphone

Equipment requirements

Note: The equipment list includes some specific brand and model components. If you are substituting another brand or model, be sure to test the activities that use those components to determine if any of the steps need to be modified.

Each student should have access to the following list of equipment:

- A notebook or other paper to record information
- Two lamps
- X10 module
- X10 ActiveHome Pro two-way PC interface
- Audio/video sender and receiver model VK80A
- X10 control unit
- Wireless network card
- Wireless access point/router
- CatX cable stripper
- RJ-45 punchdown tool
- Roll of Cat5 cable
- RJ-45 plugs
- Portable battery powered AM/FM radio (with working batteries)
- Music CDs (if possible, provide CDs with contrasting sounds such as hard rock, classical, ballads)

- Speakers and/or headphones for PCs
- TV with antennae and S-video connector
- Commercially recorded DVD
- Stereo system composed of:
 - Multi-channel amplifier
 - CD player
 - 5 speakers and a subwoofer
- 18 RCA connector cables or cables compatible with stereo system components
- DVD player
- S-video cable
- DVD movies (if possible one with dark scenes and one that is brightly lit)
- X10 MS10A motion sensor
- X10 RF transceiver model RR501 or TM751
- AA, AAA, or 9V batteries as needed for each X10 motion sensor
- X10 wireless camera system model WVK54 or equivalent (includes wireless video camera, wireless receiver, and power supplies)
- Telephone line with RJ-11 connectors
- Telephone wire (two pair Cat 3 flat or round)
- Phone jack splitter
- RJ-14 jacks
- Fax machine
- Telephone with RJ-11 jack
- Telephone with RJ-14 jack
- Cable stripper
- Flat blade screw driver
- Phillips head screwdriver
- Access to a PBX (DataLabUSA model S-308 or similar)
 - two phone extensions
 - three RJ-11 patch cables
 - one working phone line
- X10 wireless remote controller (model 4000 remote and base or similar)
- Two X10 plug-in control modules (model 2000 or similar)
- X10 mini timer controller (model 1100X or similar)
- Thermostat (standard or automated)
- Single-strand insulated wire
- X10 Model VK80A A/V sender and receiver
- Automatic thermostat (Dayton Fuel Trimmer model T-110 or similar)

First-time setup instructions

The first time you teach this course, you will need to perform the following steps to set up each student computer.

- 1 Install Windows XP according to the software manufacturer's instructions. You can perform a default installation. You can also use Windows 2000, although the screen shots in this course were taken using Windows XP and students' screens might look somewhat different.
- 2 Download an evaluation copy of Avast Home Edition from www.avast.com. You can place this on the instructor's machine in a shared folder.
- 3 Download the Active Pro Home software using the email link provided when you purchased the product. Place this in a shared folder on the instructor's machine.
- 4 Download the software for any other X10 components you purchased that require software. You will receive an email link to any software that is required. Place this software in the shared folder on the instructor's machine.
- 5 Install Adobe Acrobat Reader according to the software manufacturer's instructions. You can use the default installation options.
- 6 Create Internet accounts for the students. Students will need Web access.

Setup instructions for every class

Every time you teach this course, you will need to perform the following steps to set up each student computer.

- 1 Disconnect any devices that were set up during the course.
- 2 Reset equipment to default settings.

Downloading the PowerPoint presentations

If you don't have the CD that came with this manual, you can download the PowerPoint presentations from the Course ILT Web site. Here's what you do:

- 1 Connect to www.courseilt.com/instructor_tools.html.
- 2 Click the link for CompTIA to display a page of course listings, and then click the link for CompTIA DHTI+ Certification.
- 3 Click the link for downloading the Presentation files, and follow the instructions that appear on your screen.

Topic D: Support

Your success is our primary concern. If you need help setting up this class or teaching a particular unit, topic, or activity, please don't hesitate to get in touch with us. Please have the name of the course available when you call, and be as specific as possible about the kind of help you need.

Phone support

You can call for support 24 hours a day at (888) 672-7500. If you do not connect to a live operator, you can leave a message, and we pledge to return your call within 24 hours (except on Saturday and Sunday).

Web-based support

The Course ILT Web site provides several instructor's tools for each course, including course outlines and answers to frequently asked questions. To download these files, go to www.courseilt.com/instructor_tools.html. For additional Course ILT resources, including our online catalog and contact information, go to www.course.com/ilt.

Unit 1

Introduction to DHTI

Unit time: 60 minutes

Complete this unit, and you'll know how to:

- A** List features, functions, and benefits of DHTI systems.
- B** List basic components of DHTI systems.
- C** Identify information needed by technicians to design and install DHTI systems.
- D** Identify benefits of installation verification; deliver manuals and documentation.

Topic A: Digital home technology integration

What is digital home technology integration?

Explanation



Digital home technology integration (DHTI) is the concept of a connected home environment in which a central computer system, programmed or otherwise directed by the homeowner, manages and distributes incoming and outgoing Internet and audiovisual (A/V) digital data, and controls the network, appliances, security, and utilities of the home.

DHTI management and control can be minimal or extensive, depending on the preference of the individual and the amount of investment in equipment and infrastructure. A complete DHTI system requires a variety of subsystems, which are linked together and centrally controlled, but some degree of DHTI can be accomplished with individual control modules linked to various devices and appliances in the home. Exhibit 1-1 shows a diagram of a large DHTI system with arrows indicating the bidirectional flow of data to and from the various subsystems. Note that data flowing outside the network must pass through the gateway that protects the LAN from outside attacks and from the release of unauthorized information.

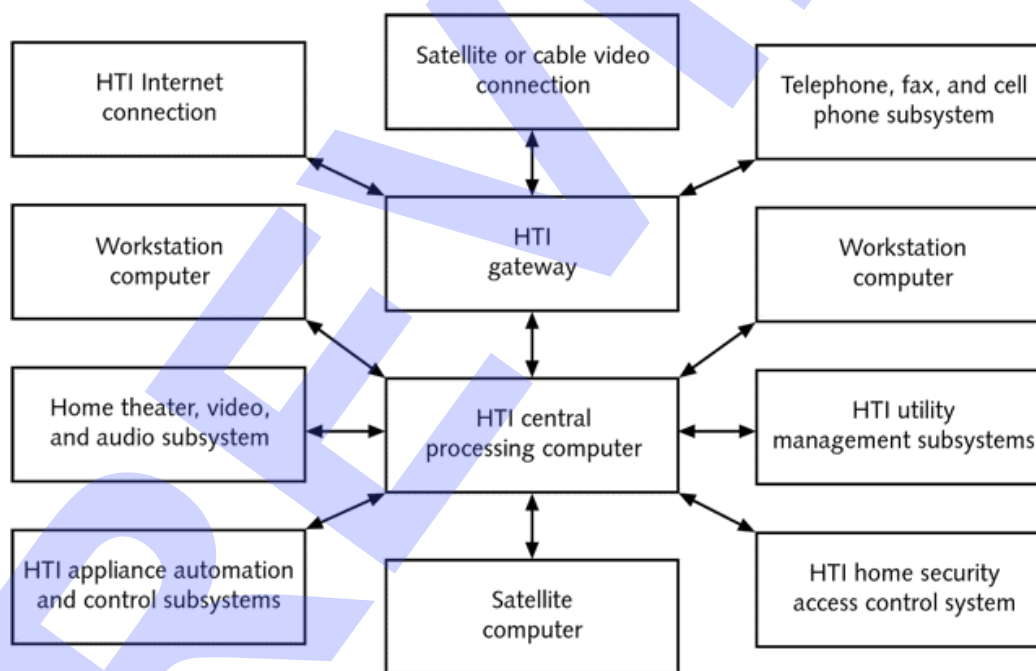


Exhibit 1-1: Block diagram of a large DHTI system



DHTI systems are generally used to provide, manage, and control six broad areas of the home technology environment:

- Internet and network (within the home) connectivity
- Video and audio signal reception and distribution
- Telecommunications
- Home security and access control
- Utility management (electricity, heat, air conditioning, and water)
- Appliance automation and control

Consumer demand for DHTI systems that incorporate some or all of these features is increasing. In order to provide the needed services, homes require a complete, automated home control network that integrates the computer-based systems with entertainment, heating and cooling control, water management, home security, and other systems.

The complexity of networking a variety of electronic products into one home control network calls for trained home networking and integration professionals who are skilled in the design, installation, and troubleshooting of DHTI computers, infrastructure, and subsystems. Consumers who employ DHTI professionals want to be assured of their technical qualifications in the field. To help provide this assurance of competence, the industry has developed a credential called CEA-CompTIA DHTI+ Certified Professional.

The CEA-CompTIA DHTI+ Certified Professional credential is designed for technicians who install and network digitally based security, audio and video, computer, heating and air conditioning, cable and satellite, and telecommunications systems.

CEA-CompTIA DHTI+ was developed jointly by CompTIA (www.CompTIA.org) and Consumer Electronics Association (www.ce.org) in response to the growing need for qualified technicians to install, service, and maintain the following digital home products:

- Communications network
- Entertainment network
- Security network
- Home control network
- Services and subscriptions
- Commercial wiring and cabling
- Ethernet, token ring, or other LAN topology

This course is designed to prepare technicians to pass the CEA-CompTIA DHTI+ exam and become credentialed as a CEA-CompTIA DHTI+ Certified Professional.

Do it!

A-1: Identifying features of digital home technology integration

Questions and answers

- 1 Provide a one sentence summary defining DHTI.

A connected home environment in which a central computer system, programmed or otherwise directed by the homeowner, manages and distributes incoming and outgoing Internet and audiovisual digital data, and controls the network, appliances, security, and utilities of the home.

- 2 List the six areas of DHTI environments.

Areas include:

- *Internet and home network connectivity*
- *Video and audio signal reception and distribution*
- *Telecommunication*
- *Home security and access control*
- *Utility management*
- *Appliance automation and control*

- 3 The CEA-CompTIA DHTI+ Certified Professional certification is designed for technicians who do what?

Install and network digitally based security, audio and video, computer, heating and air conditioning, cable and satellite, and telecommunications systems.

- 4 List some of the features that a DHTI technician might be asked to install and maintain.

A networked home entertainment, environment, and security systems, including the integration and distribution of:

- *Communications network*
- *Entertainment network*
- *Security network*
- *Home control network*
- *Services and subscriptions*
- *Commercial wiring and cabling*
- *Ethernet, token ring, or other LAN topology*

What can a DHTI system do?

Explanation

This section takes a closer look at the particular data and services a DHTI system can provide for a home and its occupants. No single DHTI system would likely include all the features described here. Although each system's parameters reflect the individual needs and wants of its owner in the data and services it provides, all the functions noted here are currently available and new ones are being developed continuously.

Internet connectivity

An Internet connection gives the home access to the World Wide Web (WWW) and to literally millions of sites on every imaginable, and some unimaginable, subjects. Home connection to the Internet is often by means of a modem connected to a telephone line. The telephone line connects the home user's computer to a service provider who, in turn, connects it to the Web. A standard telephone line connected through a modem serves adequately for most casual home users of the Internet, but it has limited data-carrying capacity. For this reason, many users lease a larger capacity Digital Subscriber Line (DSL) or use a cable modem for their Internet service. These types of connections cost more than the regular telephone link, but provide correspondingly greater transmission capacity (bandwidth).

The Internet connection from the home computer to the service provider is an important part of the DHTI configuration because the type and capacity of that connection influences how the DHTI system distributes and uses Internet data. When the home LAN has Internet connectivity through a gateway or directly to the main network computer, either of these devices can perform the following specific tasks on the incoming data:

- Scan the data to detect viruses, which can then be blocked from entering or affecting the system.
- Detect illegitimate attempts by outsiders to "hack" into the user's computer system and prevent them from accessing any information on the system behind its firewall.
- Distribute Internet access to other computers within the home by using a network setup.
- Block or password-protect access to some Internet sites, either on all computers on the network or on specific units designated by the system administrator.
- Manage all of the services available through Internet access, including e-mail, chat rooms, home or business Web sites, and so on.

Within the home, a central processing computer can also manage network services for other computers and peripherals connected to the system. A home network permits all connected computers to swap data directly, share files, use common printers, play games, and more. Maximum use of computer resources is achieved along with maximum speed of communication within the network environment.

Audio and video reception and distribution

Incoming video data usually comes to the home via cable hookup or satellite transmission. Cable television requires a direct wire connection to the transmission facility. Most, but not all, areas of the country now have access to cable connection and the number of (mostly rural) areas that don't have cable is declining as the cable providers' wiring networks expand.

Satellite television access is available nationwide because the signal transmissions originate from several satellites positioned in geosynchronous (stationary in relation to the ground) orbits in space above North America. The satellites downlink (transmit) a coded audio/video signal to a dish receiver mounted on the home and aimed directly at the satellite.

Both cable and satellite digital transmissions must pass through a decoder or translator unit before they can be displayed on screen. The decoder is set by the service provider to decode only those channels to which the user has subscribed.

The type of incoming television signals selected by the user influences the configuration of the DHTI system that uses the signal. Cable hookups can be split and the incoming signal shared among several television displays. Each television can be set to a different channel and a recorder can record one channel while the user views another. Some cable providers require a decoder box to access some or all of the channels at each device (television or recorder). Satellite hookups require a separate decoder for each television display connected to the system.

The DHTI system that receives the decoded digital television signal can do any or all of the following with it:

- Distribute the signal to the various television receivers in the home.
- Monitor and control access to selected channels or programs on a channel for all television receivers or for selected receivers.
- Direct selected programs to recording devices for storage and later use.

Telecommunications

Telephones are the most universally installed technology in America, and a DHTI system can extend the utility and expand the functions this established service performs. The voice telephone line, which is standard in almost every home, can be made available in every room, either through hardwired extensions or through wireless technology. The latter also allows telephone service to extend into the yard so that a convenient receiver can be carried while gardening or kept near the pool.

Telephone lines also provide the Internet access point in many homes. A separate line is preferable for this purpose, although one line can provide both data and voice transmission, but not simultaneously. When a traditional phone line is used for data transmission, voice calls into or out of the home are blocked. The same is true of data transmission when a voice call is in progress.

A separate data line managed by the DHTI system provides much better Internet service and can also be used as a fax line with messages being routed to fax software in the home computer or to a separate stand-alone fax machine. DHTI systems can also use a data line as an emergency alarm line connected to the home security system. The system can be programmed to take control of the line in the event of an emergency and summon immediate assistance. Voice and data transmission service can be expanded still further by the installation of a Digital Subscriber Line (DSL), a high-speed data transmission telephone line that also has the ability to transmit voice and data simultaneously.

The security system can also be programmed to use a cell phone, which isn't subject to localized power failure or cut wires, for outgoing emergency calls. This is just one of several ways in which cell phone technology can also be integrated into the DHTI system to provide better communication service to the home.

Home security and access control

A DHTI system can provide a wide variety of security measures for the home. It allows access to the home and its surroundings and other security measures to be centrally controlled and monitored for maximum protection of the occupants and their property. All of the following security and monitoring features can be included in a DHTI system:

- Cipher locks on exterior doors. These require keypad entry of a numeric code to open, and some types can be time coded to block entry during specified hours.
- Sensors on windows and other vulnerable entry points that trigger an alarm if intrusion occurs. These can be taped circuits on the glass, laser beams, or motion/vibration detectors.
- Heat and/or motion sensors that monitor the immediate area around the home or specific traffic corridors within it and trigger an alert if anyone enters the space.
- Video surveillance cameras that monitor both exterior and interior areas of the home for intruders.
- Strategically placed pressure-sensitive pads that respond either to pressure being applied (weight) or pressure being relieved (object picked up).

Any of these sensing and monitoring devices trigger a variety of responses, including the following:

- Summon the police or other assistance, either by telephone or by radio.
- Activate an audible alarm.
- Activate additional lighting.
- Activate additional security procedures such as lockdown devices, circuit breakers, dropdown security doors, and so on.

Home automation and control

DHTI automation and control systems offer tremendous convenience and labor-saving comfort for most owners and truly essential technology assistance for certain groups, such as those with limited physical mobility and those with sensory impairment. For these groups, home automation can often be the key to living independently.

Home automation is accomplished by means of remote-controlled systems activated at will by the homeowner from a convenient location, or by systems that can be programmed on a preset schedule to self-activate at specified intervals or times. Many automation features are available, including the following:

- Centralized control of lighting throughout the house and outdoor lighting fixtures as well.
- Control of window shades and curtains.
- Control of electric appliances such as coffee makers, radios, alarm clocks, dishwashers, and more. Almost any appliance operating on standard house current can be controlled remotely.
- Control of safety systems such as swimming pool covers, driveway and sidewalk heating systems, and roof de-icing systems.
- Management of personal safety devices such as baby monitors, fall alarms, and vital sign monitors.

For persons with limited mobility, having as many home systems as possible automated and controlled from a central location is essential. If physical movement is severely restricted, control systems can often be adapted to function easily using whatever motion is available to the user or by using voice commands.



Utility and resource management

A DHTI system can help minimize energy waste, increase efficiency, and reduce costs by continuously monitoring and managing utility usage. The system can turn off lights and other electrical devices when not in use. Lights left on in a room can be turned off automatically when a sensor detects that the room is unoccupied for a preset period of time. When anyone enters the room, the lights come on again, controlled by the same sensor.

Sensors and timers can control heating and air conditioning systems. This provides maximum energy efficiency while maintaining comfortable temperatures for the home's occupants. Heat can be turned down at night and when the home is unoccupied during the day, then turned back up just before the occupants awaken or return home. Air conditioning can be similarly adjusted to fit the schedules of those in the home.

Efficient home use of water includes the controlled watering of landscaped areas, which usually requires far more municipal water than any other consumer use. By adjusting sprinkler systems to provide only the needed amount of water for each part of the landscaping, and programming them to operate after sundown and for only the necessary time, a DHTI-managed system can use less water and be far more effective in maintaining the landscaping.

A DHTI system can also assist in managing a swimming pool. An automated cover that covers the pool when not in use prevents evaporation and helps hold heat in the pool. Pool filtration systems can also be timed to clean and backflush (part of the cleaning process in most pool filtration systems) at night, and in some locations, the waste water used for these operations can be directed to the landscaping.

Do it!

A-2: Identifying functions of DHTI systems

Questions and answers

1 List the functions provided by DHTI.

Answers should include:

- Internet connectivity
- A/V reception and distribution
- Telecommunications
- Home security and access control
- Home automation and control
- Utility and resource management

2 What functions are provided by a gateway to connect the home LAN to the Internet?

Answers should include:

- Scanning data to detect viruses
- Detecting illegitimate access
- Distributing access to multiple computers within the home network
- Blocking or password protecting access to some Internet sites
- Managing all of the services available through Internet access

3 How is incoming video data usually brought into the home?

Through a cable hookup or satellite transmission

4 How do you share incoming A/V signals?

Cable hookups can be split and the signal shared among several televisions. You might need a decoder for each television if your provider requires one for accessing some or all of the channels.

Satellite hookups require a separate decoder for each television connected to the system.

5 List some of the functions provided by a telephone telecommunications line.

Answers should include:

- Voice transmission
- Data transmission
- Internet access
- Fax
- Emergency line for the home security system

6 List some of the features provided by home security and access control.

Answers should include:

- *Cipher locks*
- *Window and door sensors*
- *Heat and/or motion sensors*
- *Video surveillance cameras*
- *Pressure sensitive pads*

7 List some of the home automation and control features.

Answers should include:

- *Centralized control of indoor and outdoor lighting*
- *Control of window shades and curtains*
- *Control of electrical appliances operating on standard household current*
- *Control of safety systems*
- *Management of personal safety devices*

8 What features can be provided for utility and resource management in a DHTI system?

Answers might include:

- *Turning on and off lights so they are on only when the room is occupied*
- *Controlling heating and air conditioning so that they are adjusted to maintain comfortable temperatures for home occupants*
- *Adjusting water sprinkler systems to provide water only where needed and to use them only at certain times*

Explanation**Benefits of DHTI**

The main benefits of DHTI are simple: it makes the user's life more convenient, safer, and more fun. It provides maximum use and enjoyment of electronic media, Internet, and telecommunication systems. DHTI makes technology available where and when the user wants it. Automated systems that function on demand or by programmed direction to meet predetermined needs in a timely manner often become essential services rather than mere conveniences. Similarly, DHTI's ability to make communication and data sharing easy to use throughout a home enables users to make maximum use of technology to save time while accomplishing more. When that increased productivity is utilized in a home business setting, the payoff occurs not only in time efficiency, but in increased profitability. When technology extends the senses and physical abilities of the physically challenged, while at the same time monitoring their safety and health, it becomes a critical, life-enhancing, if not life-saving, necessity.

Technology on demand

Hardly anyone who has watched a home theater system featuring a 60-inch screen with high-definition television viewing and surround sound audio reverberating from high-quality speakers will be content to go back to a small screen with standard resolution and a single 6-inch monaural audio speaker. Similarly, no one who has come home on a snowy evening to find the driveway and sidewalks clear of ice, the garage door opening as the car's front bumper approaches it, and the house warm and brightly lit, is anxious to return to the "good old days" of snow shovels and manual lift doors. In other words, DHTI makes life a lot more pleasant and a lot less work.

Technology to save time

Users also save time with DHTI. Its automated features eliminate the need for many household tasks to be done manually and make services available on demand throughout the home with no need to move or alter equipment setups. With DHTI, each room in the house can be connected so that telephones, Internet, television, radio, and network services are all available wherever and whenever they're needed or wanted. Whole-house connectivity also means no waiting for multiple users, each of whom can log on simultaneously. The system apportions bandwidth and delivers data efficiently so that everyone can perform their desired tasks using the shared resources.

DHTI saves the user time by automating the performance of routine tasks and functions using a set of programmed instructions. With DHTI, custom programming is available that permits a very sophisticated level of control in many automated systems simultaneously. There's no need for the user to think about or perform any of these daily tasks.

Technology to save money

By taking over the management of home functions, DHTI can make them more efficient and therefore more cost effective. The automated system won't leave the water running too long or forget to turn off the lights when rooms are empty. It always turns down the heat or the air conditioning at night and activates the security system to make sure the occupants' rest is undisturbed. Standardizing household functions for time of performance and duration minimizes the amounts of energy and resources these operations use, which saves the homeowner money.

A sprinkler system can be programmed to water the yard from midnight until 3:00 a.m. on Mondays, Wednesdays, and Fridays from April 15 to October 15, and also add a Saturday or Sunday watering whenever the preceding five days include two or more with daily high temperatures above 90 degrees. Operating on those instructions, the DHTI system can keep the yard green throughout the spring and summer. The homeowner may never see any evidence of the process and probably won't need to alter or adjust it unless there's a breakdown in the equipment.

Assisted living functions

DHTI can provide genuine security for the home and the family living in it. With that security comes a feeling of peace and comfort that's hard to quantify in monetary terms. DHTI security can protect people and property not only against break-ins, burglaries, and other criminal activity, but also against the danger of fire, electrical malfunctions, and water damage. The system can alert the homeowner to danger and quickly summon assistance. It may also be able to shut down faulty power circuits, close gas valves, or activate sprinklers to help control a fire.

DHTI can also provide some protection for children. The protective devices include individual cell phones or location monitors that children can carry with them. They also include protective devices such as security gates and pool covers, and quick, easy access to communication links that they can use to get help in the event of an emergency. Similar systems can be set up to monitor the welfare of individuals in customized ways so that assistance is automatically requested if any injury is suffered or a health-related problem occurs.

Home office enhancement

Whether someone is operating a small business or telecommuting to a distant office or other location, DHTI benefits the person working from a home office. DHTI makes maximum services and functions available for business use just as it does for home use. Some of the costs of DHTI can be taken as business expenses if they're used in a home office, and some services whose cost can't be justified for home use only become economical when their use is shared among personal and business functions.

DSL, for example, which is usually provided at a fixed monthly cost regardless of the amount of use, is often required for business use in a home office. After hours and on weekends, when the business use of the line is minimal, the family can make use of the line.

Do it!

A-3: Identifying benefits of DHTI systems

Questions and answers

- 1 What are the three main benefits of DHTI?

It makes the user's life more convenient, safer, and more fun.

- 2 List some examples of technology on demand.

Answers might include home theater systems, driveway clearing, garage door openers, and light and heat systems.

- 3 List some examples of how technology can save time.

Answers might include automating manual tasks, making services and features available throughout the home so users don't need to wait their turn, and pre-programming instructions for routine tasks and functions.

- 4 List some examples of how technology can save money.

Answers might include turning off water and lights when they are not needed, adjusting room temperature for day/night, programming sprinkler systems to water at specific times under certain conditions.

- 5 List some of the ways a DHTI system can provide assisted living functions.

Answers might include security from break-ins; protection from fire, electrical malfunction, and water damage; location monitors for children; protective devices such as security gates and pool covers; and automatic request for assistance if a person is injured.

- 6 What are some of the benefits of DHTI for home offices?

Answers might include the same benefits as for home use; DHTI costs as a business expense and helps justify the expense; sharing high capacity Internet service with the family after hours.

Topic B: Basic components of DHTI systems

DHTI system components

Explanation

Although DHTI can be used for an almost endless variety of data functions and control of devices and operations, all automated home technology systems consist of combinations of six basic components:

- Processors
- Communication links
- Sensors
- Control devices
- Display and monitoring devices
- Recording and storage devices

A desktop or laptop computer contains all six of these components and is, therefore, an example of an integrated technology system. Exhibit 1-2 shows a diagram of a computer system with several input and output devices sending information to and receiving information from the central processing unit, which is the “brain” of the system and performs all the manipulation of its data.

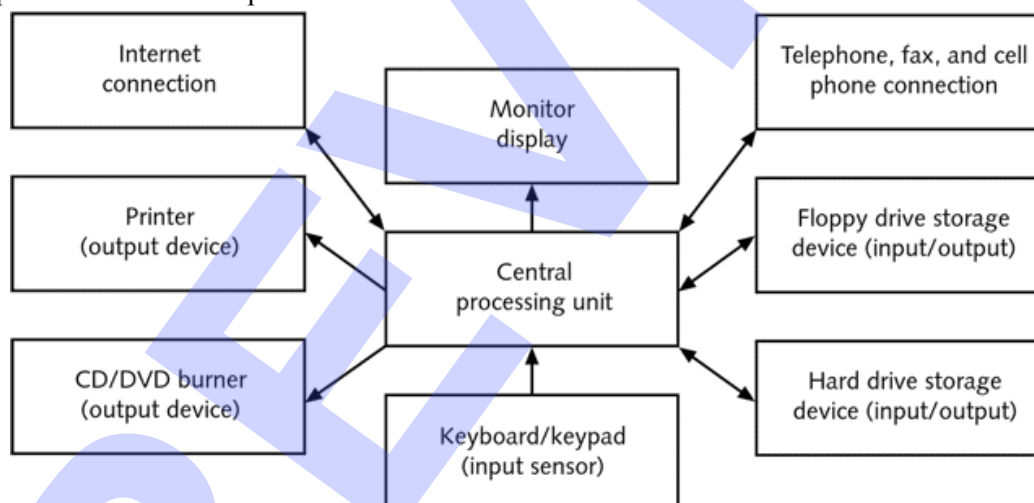


Exhibit 1-2: Computer system block diagram

DHTI simply expands the scope and the scale of components so that their functions can be extended over a wider geographic area—the whole interior and exterior of a home and its surrounding yard—and to a much larger array of output and storage devices than just the computer’s display screen and its hard drive. Exhibit 1-3 shows a small DHTI system that extends the input and output reach of a computer by providing it with input from other segments of the home LAN and allowing the central computer to remotely control automated systems in distant segments of the LAN.

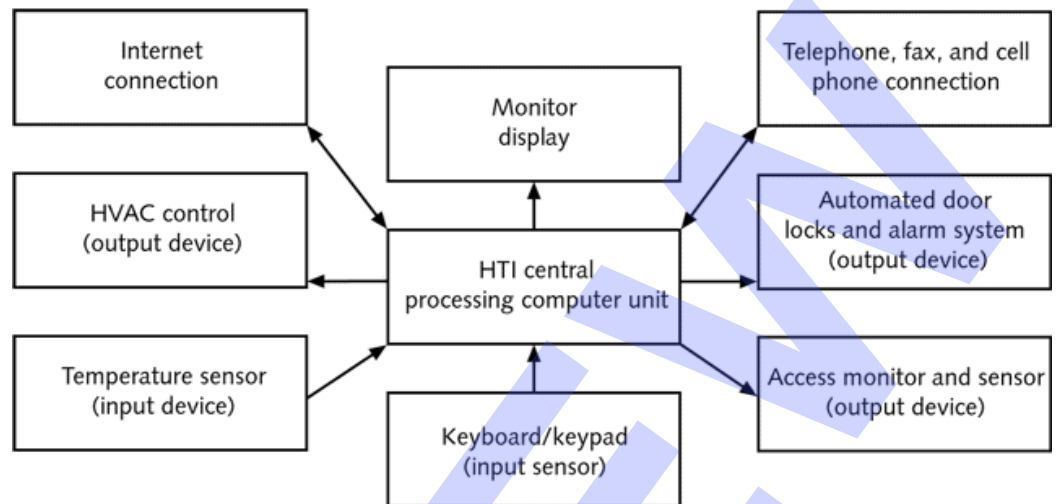


Exhibit 1-3: Block diagram of a small DHTI system

Processors

Processors are electronic devices that receive digital information (input), process this information according to a set of stored instructions (program), and send the results of their processing (output) to another device that can display it, store it for future use, or perform a preprogrammed action by using the information or based on it.

A computer's central processing unit programmed with word-processing software constitutes a processor. It receives input data from the keyboard, processes the input according to its programmed instructions into a finished document, and sends the results to a printer, which displays the data as a printed page.

In a DHTI system, a processor may receive many different types of input from a variety of input devices such as cameras, sensors, microphones, telephone links, and so on. The input data may be processed in a variety of ways, according to the manner in which the processor has been programmed, and the results of that processing may be output to various storage, display, and action devices in equally diverse ways.

Input to a processor, for example, could come from a digital thermometer, which is one type of temperature sensor. If the sensor sends data to the processor that the outside air temperature has fallen near the freezing point of water, the processor might compare the temperature information it receives with a preset schedule of instructions and, as a result, output instructions to subsystems throughout the home. It might send instructions to perform any or all of the following actions:

- Shut down the sprinkler system.
- Cover the swimming pool.
- Turn on the driveway heating system.
- Turn on the rain gutter de-icing system.
- Close vents and windows in the home.
- Turn on the space heater in the doghouse.

In DHTI, a single central processing unit is usually sufficient to operate and control the entire system, although some subsystems may have smaller processors to perform localized functions. Centralized processing permits the greatest degree of integration among all subsystems and helps ensure that they aren't acting in conflict with one another. It would be counterproductive, for instance, to have one automated function turn on the air conditioning system, while another opened windows and vents to the outside at the same time. If one processor controls all automated functions, its programming can be integrated for maximum beneficial effect.

Communication links

Communications links are the infrastructure of an integrated technology system and work to tie that system together as a functioning unit. These links are the wires, cables, connectors, wireless transmitters, receivers, routers, switches, and other devices that connect the components of a system and permit them to transmit and receive data both among themselves and to the outside world.

These bits and pieces of hardware and lengths of wire are usually quite simple and mundane objects, but they are critically important parts of every integrated technology system. Correctly designing, installing, and maintaining communication links can do more to ensure the reliability of an integrated system than any other facet of the system's creation.

In a computer, all of whose components are housed in a single case and closely wired together, communication links are made up of the integrated circuit boards, buses, sockets, and cables that connect the parts electronically so that data can be transferred among them. DHTI systems use similar links, but because their components are usually farther apart, the communications links are longer and need to be more robust. Because they are usually built-in as part of the home's structure and are difficult and expensive to repair or replace, the cables, connectors, plugs, and other infrastructure of a DHTI system must be durable over time and able to resist the effects of weathering, outside interference, and other factors that can degrade their performance.

DHTI communications links can be hardwired using a variety of cable types and sizes and suitable end-point connecting devices. Hardwiring is performed most conveniently and at the least cost as part of the construction process when a home is built, but it can be done after the home is completed using a process called retrofitting. Retrofitting a home for DHTI may cost more than new construction wiring and may be less pleasing in appearance because of the difficulty of entirely concealing wiring and connectors after the finished surface of the home is complete.

Wireless connection of DHTI is often preferred for retrofitting existing homes and even for some new construction. There are several wireless technologies that can provide connectivity for a DHTI installation. Most require the installation of one or more radio transceivers within the home, which communicate with all the components of a DHTI system via high-frequency radio transmissions. No wiring is required for this type of installation except a power connection for the transceivers (hubs) and hardwired connections for Internet and television data coming into the home.

At least two other technologies, the X10 system and the Home Plug system, use the existing electrical wiring in the home to carry digital data in addition to the standard electric current flowing through these circuits to power lights and appliances. Still another technology, called HomePNA, also requires no new wires to be installed in the home because it uses the existing telephone wires to carry data to devices on the home network.

Sensors

Sensors are devices that convert human activity or environmental conditions into data. A keyboard that reacts to finger pressure on each of its keys is a type of sensor. It senses pressure applied to each key and converts it into corresponding digital data, which goes to the computer's central processing unit. A microphone is another type of sensor that reacts to the air pressure of sound waves and converts voice commands or dictation into digital data for the computer.

Sensors in a DHTI system can be the same keyboard, microphone, or mouse found in any computer system. They can also be other much more diverse devices and they can be separated by much greater distances from the central processor to which they send their data.

In a DHTI system, keypads can be located near the home's entrances where they serve as input devices for the codes to open cipher locks on doors. Other keypads can be located throughout the home and may control entertainment systems, lighting, curtains and shades, garage doors, and others functions.

Environmental sensors are devices that react to some aspect of conditions around them. A temperature sensor, for example, continually sends the current temperature to the processor, which then determines whether to adjust heating, air conditioning, or other systems, based on the data it receives.

A light sensor measures the light level in a room and sends the data to the processor, which can turn the lights in the room off, if another sensor indicates the room is unoccupied. Alternatively, the processor may open window shades and curtains to increase a low light level during daylight hours. A light sensor placed inside a normally dark cabinet or case can even be used to shut down a system for safety reasons or trigger a security alarm if the door to the cabinet is opened, letting in light. Exhibit 1-4 shows a diagram of a lighting control segment of a home LAN, including sensors to detect interior and exterior light levels and control modules to adjust shades, curtains, and lighting both inside and outside the home. Arrows show the direction of data flow to and from the various devices. From the keyboard, the LAN administrator can program the system parameters and set any of its features by time, as well as by sensor input.

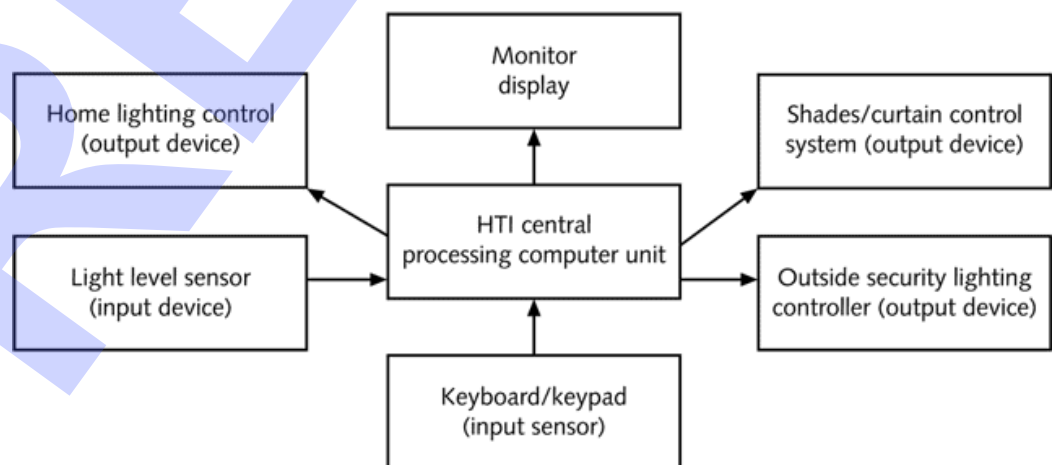


Exhibit 1-4: Block diagram of a light control segment of a home LAN



Other types of sensors include the following:

- Smoke detectors
- Heat (infrared) sensors
- Motion (vibration) detectors
- Pressure or weight pads
- Water level sensors
- Chemical sensors such as carbon monoxide monitors

All of these devices send data to the processor about the particular environmental condition that they monitor. The processor compares this information to its programmed instruction set and directs the system to respond accordingly.

Control devices

Sensors collect information about conditions around the house and send it to the processor. The processor evaluates that information and issues commands to the appropriate control devices. These devices are the action components in a DHTI system. They act on the processor's instructions to turn off, turn on, or adjust the level of subsystems in the home.



Control devices come in many forms:

- Switches, which turn electrical appliances on or off
- Electromagnetic valve controls in water systems
- Magnetic lock controls
- Electrical relays, which act as switches in circuits
- Electromagnetic mechanisms that perform linear movements such as pulling curtain and shade lines or drawing a pool cover open or closed

All control devices in a DHTI system have the ability to receive digital instructions from a processor and convert those instructions into some form of action or movement. Many control devices can also be operated manually so that the instructions they receive from the processor can be overridden, and the subsystems they control can be operated or shut down on site in the event of an emergency or a system failure.

In some cases, you can have an LCD panel installed from which the homeowner can control functions. It might be configured to allow control of audio and video systems, lighting, temperature, and security systems.

Display and monitoring devices



Display and monitoring devices are usually computer screens or television screens that display video and audio signals brought into the home via the Internet, by cable, or from satellites. They also display software programs running on home computers, recorded programs from video recorders and DVDs, and data generated by the processor about the status of other systems throughout the home.

Speakers and earphones are audio devices that “display” sounds to our ears. They play the music of recorded CDs, allow users to speak with one another in separate parts of the home, and output the conversations of audio chat rooms. The processor can also use speakers to sound warnings or alarms if the DHTI system detects danger or other problems within its programmed parameters.

Note: Other types of monitoring devices include continuity lights, which monitor circuits, and space monitors, which can use motion, heat, or pressure sensors to monitor a given area.

Distribution panel

A distribution panel enables the homeowner to control integrated systems from a single location. This can be for a single system, such as an audio/video system or security system. Some other distribution panels give access to multiple systems such as audio/video; security; telecommunications; computer network; heating, ventilation, and air conditioning (HVAC); water control; and lighting systems.

Recording and storage devices

Recording and storage devices save digital data so that it can be retrieved and used again. Computers typically store their data on magnetic devices such as hard drives, floppy disks, Zip disks, tapes, and memory sticks.

CDs are storage devices that store data in a form readable by a beam of light reflecting off the disc as it spins in a player. Television programs and movies are usually stored on videotape cassettes and DVDs by recorders, which can also play these devices to recover and display the data.

Entertainment programs, video and audio, will nearly always be on videocassettes, CDs, or DVDs. These media can also record images from security cameras and other monitors in the DHTI system. Storing images and data from system monitors, especially those devices in the home's security subsystem, allows any significant event to be reviewed after the fact, often a critical advantage in investigating crimes or settling disputes. Home residents can use recorded data to determine the time and date of events that occurred while no one was at home.

The type and amount of data to be stored usually determines the type of device used. Video programs and high-resolution photographic images are the most data-intensive types of files, and so usually require the largest capacity storage devices. Next in size are sound files followed by graphic files. The smallest files are usually those composed of text or numerical data.

Do it!

B-1: Identifying components of DHTI systems

Questions and answers

- 1 List the six basic components of an automated home technology system.

Components include:

- **Processors**
- **Communication links**
- **Sensors**
- **Control devices**
- **Display and monitoring devices**
- **Recording and storage devices**

- 2 A personal computer is an example of an integrated technology system. True or false?

True

- 3 Is it more beneficial to have a single central processing unit or one in each subsystem? Why?

It is best to have a single central processing unit to ensure the greatest degree of integration and that the subsystems are not acting in conflict with one another.

- 4 Which component ties the integrated technology system together into a functional unit?

The communication links

- 5 List examples of sensors that might be incorporated into a home technology system.

Answers might include:

- **Keypads for locks, control of entertainment systems, lighting, window coverings**
- **Environmental sensors that send temperature information to the central processor**
- **Light sensors to activate lights in a room or cabinet**
- **Smoke detectors**
- **Heat (infrared) sensors**
- **Motion (vibration) sensors**
- **Pressure or weight pads**
- **Water level sensors**
- **Chemical sensors such as carbon monoxide monitors**

6 What are control devices?

The action component of the DHTI system that acts on information received from the processor

List examples of control devices.

Examples include:

- ***Switches to turn appliances on or off***
- ***Electromagnetic valve controls in water systems***
- ***Magnetic lock controls***
- ***Electrical relays***
- ***Electromagnetic mechanisms that perform linear movements***

7 List examples of display and monitoring devices.

Answers might include:

- ***Computer monitors and televisions***
- ***Speakers or headphones***
- ***Continuity light***
- ***Space monitors***

8 What is an advantage of having recording and storage devices incorporated into a DHTI system?

Storing images and data from system monitors allows events to be reviewed after the fact, which can be a critical advantage in investigating crimes or settling disputes.

Do it!

B-2: Researching DHTI products on the Internet

Here's how	Here's why
1 Open your Web browser and connect to the Internet	You will search for sources of home automation hardware and locate specific items.
2 Using a search site, search for the phrase "home automation"	You can use the browser's search function or connection to a search site such as Google, Yahoo, or any site of your choice.
3 Record the URL of at least three companies that sell home technology integration products	<i>Answers will vary.</i>
4 On each of the vendor sites you located, find a device that remotely turns a lamp or other electrical device on or off via remote control	
5 Compare the cost and features of each device, and then determine which you would buy to install in your own DHTI system	



You can provide students with notebooks to record their findings or have them enter notes in a Notepad document.

Do it!

B-3: Finding components for a control system on the Internet

Here's how	Here's why
1 In the Web sites you recorded in the previous activity, locate the additional components you need to make the device fully functional	You will find what other components are required to make the control devices you found in the previous activity functional, determine costs, and decide which complete system is the best value.
2 Make a list of the items needed for each device along with prices	
3 Add up the subsystem prices for each of the devices	
4 Did the total cost of the subsystem change your mind about which device to buy (compared to your decision in the previous activity)? Why or why not?	

Topic C: Designing and installing DHTI systems

DHTI professionals

Explanation



The need for professionals skilled in integrating home networking equipment is growing as a direct result of rising consumer demand for home networking products and Internet-enabled devices for entertainment, voice, and data systems. Homes with complete, automated control networks that integrate computer-based systems together with entertainment, heating and cooling, water management, home security, and other systems are being constructed or retrofitted in growing numbers.



The CEA-CompTIA DHTI+ certification is designed for technicians who install and troubleshoot integrated residential subsystems, beginning from the demarcation (d-mark) point, which is where the homeowner's network equipment and the external network service provider's equipment meet, to where the regulated signal stops.



The CEA-CompTIA DHTI+ Certificate is a cross-industry credential providing recognition that a Digital Home Technology Integrator (DHTI) professional has attained a standard of excellence in the integrated home networks industry. The certification is based on a set of standards designed to measure the knowledge and understanding of core competencies regarding the installation, integration, and troubleshooting of the following subsystems:

- Home security
- Audio and video
- Computer networks
- HVAC systems
- Cable and satellite
- Broadband
- Telecommunications
- Service provider wiring (external)

How much DHTI is enough?

The answer to this question is about the same as the answer to the question: How much equipment should mountain climbers carry? Enough to reach the summit they're ascending, but not so much that carrying it is a burden. Similarly, a home technology system should provide the entertainment, communication, and automation the user needs and wants, but should not be so expensive that its cost outweighs its usefulness, nor so complex that the home owner finds it difficult to use or maintain.

There is no ideal DHTI system. Each installation is a balance between features and costs. Each person has his or her own preferences about how many subsystems a DHTI design should have and what features and level of performance each of them should have.

With that said, it's evident that the first major step in creating a DHTI system is to develop an overall design. The design should start with a list of objectives describing what the system should be able to deliver in data and services, and what it should be able to do in automation, monitoring, and control.

Specific, detailed objectives allow DHTI technicians to design a system in the most economical way. Of course, when planning for wiring or wireless installation, whether in new construction or as a retrofit, it's a good idea to design for more capacity than you think you'll need. Doubling the required number and capacity of communication links over what the design indicates are actually needed is generally a good investment in the future. The reasons for building in such excess capacity are twofold:

- First, installing wiring and other infrastructure in the walls of a home is the most difficult and expensive part of creating a DHTI system, but installing multiple wires requires very little additional effort and costs very little more. The wire and other hardware parts aren't expensive. It's the labor of stringing and pulling them through finished walls that takes time and costs dearly. Hence the axiom: Never pull a single wire; always double it. Even if you have no need for the second wire at present, chances are good that you will later.
- The second reason is that when the user sees how useful, how convenient, and how essential DHTI can be in the American home, the system as originally designed may begin to seem inadequate. To many DHTI consumers if some is good, more is better.

Do it!

C-1: Designing a whole-house lighting control system

Here's how	Here's why
1 Open your Web browser and connect to the Internet	You will explore a Web site and design a full DHTI light control subsystem.
2 Access a site selling home automation components	You recorded several of these in an activity in the previous topic.
3 Locate the components for a complete home lighting control subsystem	
Determine how the components connect together	
4 Determine how the components can interface with the home lighting	Be sure to plan for necessary central control station and wiring or wireless technology needed to connect it with the control devices on the home's lights.
5 Determine the price of the system	Record this information in your notes.
6 Estimate the number of hours it will take you to install the system	
Determine the cost of your labor at \$20.00 per hour	
Add the cost of materials and labor costs to determine the complete lighting control subsystem cost	

Internet service availability

Explanation

There are more options than ever for connecting to the Internet. The Internet service providers (ISPs) vary from location to location. Various ISPs offer different features. They are constantly upgrading their services and equipment to provide users with the fastest and most reliable connections possible.

Telephone lines connected to modems still is a viable option for those locations that have telephone service but do not have cable or DSL access. If there is no telephone line there is also the possibility of using satellite or cellular technologies to connect to the Internet.

Cable and DSL access provide the fastest connection transfer rates. Another advantage of using this technology over telephone lines is that the technology doesn't tie up your voice line or require a second telephone line to be installed.

Do it!

C-2: Determining the availability and cost of Internet service in your area



If you want students to use a different search site, check that the syntax listed works in your choice of search engine.

Here's how	Here's why
1 Open a Web browser	You will determine the availability and cost of Internet service from providers in your area.
2 Open Google.com	
3 Search for the phrase "Internet service provider"	You will probably receive more than a million responses.
4 Refine your search by adding the state and town where you are located	For example, "Internet service provider" +Rochester +NY.
5 Determine if any of the providers listed offer nationwide service	
Determine if any of the providers listed offer only local service	
Determine the cost for the service	You can contact them or locate information online.
6 Compare the features offered by each service in relation to the cost	Discuss this with your classmates.
Determine which ISP offers the best Internet service for your needs	

Topic D: After the installation of DHTI systems

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
6.3	List and describe the benefits of verification of installation. <ul style="list-style-type: none">• Properly label wires• Wire mapping• Importance of documenting work upon completion<ul style="list-style-type: none">• Input/output verification for all systems• Document wire placement• Certification of cable installation
6.4	Deliver appropriate manuals and documentation to the end user upon completion of installation. <ul style="list-style-type: none">• Select, archive, and appropriately distribute critical system information: passwords, access codes, user IDs, credentials, and so on.

Properly labeled wires

Explanation

You should properly label all wires. This will be important if moving, upgrade, or repair of the system components becomes necessary. Proper labeling will make it a much simpler task to reconnect or reconfigure the system.

Wire mapping

Wire mapping entails mapping the route of the wires in each room in addition to tagging the wires themselves on a floor plan. Using color as well as titles for each wire will keep the diagram easy to read. This should include all of the wires such as network cabling, security system cabling, and wiring for any other home integration system components.

Importance of documenting work upon completion

The best time to document the work is as you are pulling the wiring or when you finish the installation for each room. This is because the room layout will be fresh in your mind and confusion with other room layouts will be unlikely.

Before starting installation, it is a good idea to diagram the home wiring noting the location of all wiring runs, wiring closets and pipe chases, the range of wireless networks, and the LAN connections will be located. The diagram can be best drawn as an overlay on a schematic diagram of the home and surrounding yard that shows the location of existing electrical wiring and other circuitry as well as the basic construction of the home. A typical diagram of home wiring is shown in Exhibit 1-5.

D

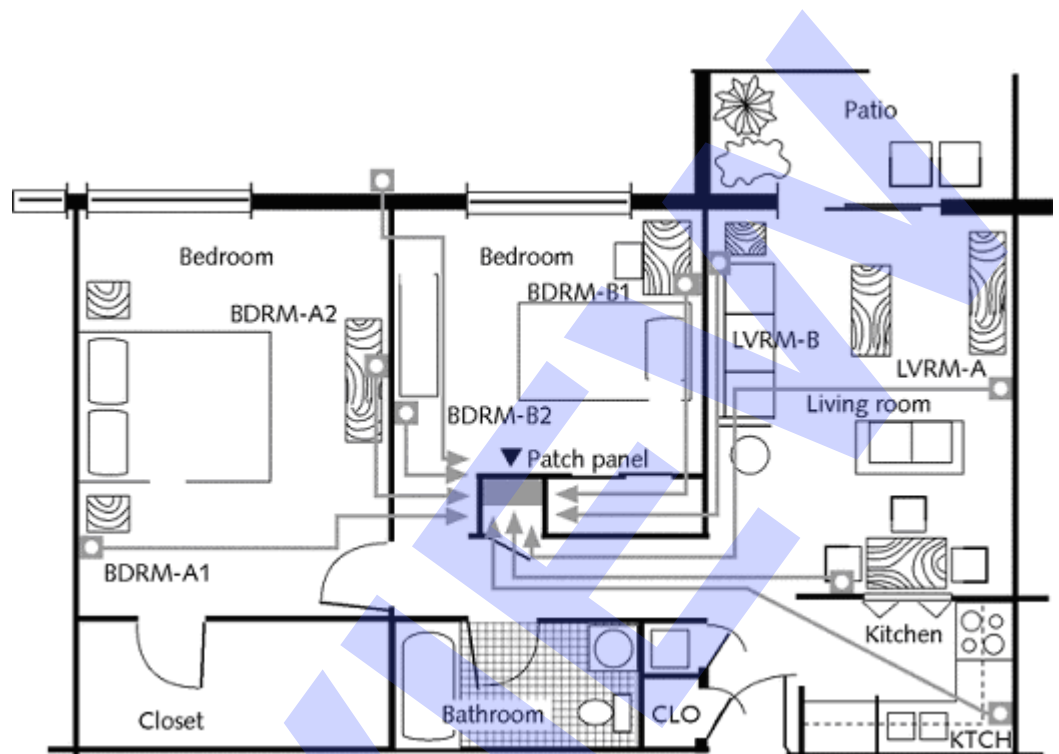


Exhibit 1-5: A wiring document

As shown in Exhibit 1-5, note the location of all the network nodes and, very specifically, the location of each of the wall jacks by which they connect to the network. If you plan to have part of the network running on technologies other than Ethernet, also note where the devices for these technologies are located and, if they require AC power, how they connect to it. If you use wireless, HomePNA, HomePlug, or X10 segments in the network, you want to connect them at some point to the Ethernet. The most convenient place to do this is usually near the patch panel and gateway setup.

The first priority is to select a location for the patch panel and other equipment in an unfinished area of the home, if at all possible. All the wiring comes into the patch panel and fishing all of them through finished walls enormously increases the labor of installing the network. It is far better to work in an unfinished area.

The second priority for the location of the patch panel is to find the (unfinished) place in the home that is most conveniently situated for pulling wire from all the other areas of the home where nodes will be placed. This likely won't be a distant corner of the building, but someplace more centrally located. Under stairs, in a utility (furnace) room, or in a centrally positioned closet are all good possibilities. All of these are likely to have good access to the basement or attic, both places through which much of the wiring can easily run. In a two-story home, these are also the areas most likely to provide access from the lower to the upper floor. If these areas don't have access already, holes to provide it can be cut or drilled in the unfinished floor beneath and ceiling above. These access points can later be covered with finished wallboard or cabinetry when the wiring infrastructure is in place.

Once you have the patch panel location set, note it on the diagram and then plan where the cables will run from each jack to the patch panel. The diagram is two-dimensional, but you have to think in three. Each cable run has to reach its destination within the length and breadth of the home, but also run up and down in the vertical dimension so that it remains concealed either within the building's structure or surface mounted on the walls. Retrofit wiring requires more cable than wiring in new construction, and there is also more waste because cable segments often have to be cut long in order to be pulled into place and then trimmed off later.

When your diagram for the network is complete, label everything on it with a short, unique designation. Start with the rooms: living room equals LVRM, master bedroom equals BRM1, and so on. The jacks in each room can take their names from the room: LVRM-A, LVRM-B, and so on. If each jack has only one cable running to it, then the cable ends can be labeled with the name of the jack. If the jack has multiple ports for data, telephone, or video, then each port must have a separate name: LVRM-A2, LVRM-A3, and so on, and the cable running to each must be correspondingly identified.

Labels are among the most critical items in the network installation process. Nothing saves more labor than accurate and complete labeling of every port and cable end. Nothing causes more frustration and makes troubleshooting more difficult than cables you can't identify running you know not where. Label everything, and use labels that stick fast and won't come off when the cable is handled and pulled through narrow openings.

Certification of cable installation

You should provide the home owner with a document attesting to the proper installation of the cables that you installed. Knowing what constitutes the proper installation of components, wiring, and modules will enable you to verify that the cabling was properly installed. A certified electrician can double-check the installation of the cables in the home. Alternatively, you could hire a Graymark Cable Installation certified inspector.

Do it!

D-1: Verifying the installation

Questions and answers

- 1 What steps should be taken to verify that the installation was successfully completed?

Verify that there is no interference, that all cable runs function properly, and that they have been properly terminated.

- 2 Who should complete the verification of the installation?

An electrician or certified cable inspector

Manuals and documentations

Explanation

After completing the installation of the DHTI components, you should present the manuals to the user. It would be beneficial to the end user to have them in a three-ring binder if possible. Place the user manuals in tabbed sections for each component. At the back of the binder in a separate section, place all of the installation manuals in the same order as the user manuals are presented in the rest of the binder.

In addition to the manuals, you should include information the user needs to access and use the components. This would include any passwords and access codes programmed for any of the components. In addition, if there are user IDs or other credentials that you configured for the user, those should be presented as well. You can present this on a sheet at the front of the binder. However, make sure that users don't leave this information in the binder. They should memorize it and either destroy the sheet or place it in a safe where it cannot be easily accessed by unauthorized persons.

Do it!

D-2: Delivering manuals and documentation to the end user

Questions and answers

- 1 Discuss why the end user might want the installation manuals as well as the user manuals for installed components.

If there is a problem down the road, knowing how the components were installed can help in troubleshooting the problem.

- 2 Why is important that the passwords, access codes, and user names and credentials not be left where they can be easily found?

All the hard work of securing the systems will be for naught if unauthorized persons gain access to this information.

Unit summary: Introduction to DHTI

- Topic A** In this topic, you identified the features, functions, and benefits of **digital home technology integration**. You learned that **DHTI** is the concept of a connected home environment in which a computer system manages and distributes Internet and audiovisual digital data, and controls the network, appliances, security, and utilities of the home. In addition, you learned that DHTI systems provide, manage, and control six areas of home technology environment: **Internet and network, video and audio reception and distribution, home security and access control, telecommunications, utility management, and appliance automation and control**. Finally, you learned that DHTI can make home life **more convenient, safer, and more fun**.
- Topic B** In this topic, you identified the basic components of DHTI systems. You learned that DHTI systems consist of combinations of six categories of components: processors, communications links, sensors, control devices, display and monitoring devices, and recording and storage devices.
- Topic C** In this topic, you identified the knowledge needed by technicians to **design and install DHTI systems**. You identified the competencies needed for **CEA-CompTIA DHTI+ professional certification**. You learned about how much DHTI is needed for a given situation. You also learned that DHTI systems should be carefully designed to accomplish the specific entertainment, data transmission, security, and automation objectives that the user desires. Provisions should be made for expanding initial designs.
- Topic D** In this topic, you identified the benefits of verification of the installation. You also discussed delivery of appropriate manuals and documentation to the end user upon completion of the installation.

Review questions

- 1 What does the abbreviation DHTI stand for?
Digital Home Technology Integration
- 2 What are the major components found in a DHTI system?
Processors, communication links, sensors, control devices, display and monitoring devices, and recording and storage devices
- 3 What are some of the areas of home automation that can be addressed by a DHTI system?
Home security, audio/video, computer networks, HVAC systems, cable/satellite connections, broadband connections, telecommunications, and lighting and electrical systems
- 4 Which of the following would not be purchased by a consumer from a service provider, as discussed in this unit?
 - A Electrical service
 - B Gas service
 - C A computer**
 - D DSL service
 - E A decoder

- 5 What groups of people can benefit particularly from DHTI's automation features?
Disabled and handicapped individuals
- 6 What are the six main areas of the home environment that DHTI systems provide, manage, or control?
Internet connectivity, audio and video reception and distribution, telecommunications, home security and access control, home automation, and utility and resource management
- 7 What is the function of a sensor?
They are devices that convert human activity or environmental conditions into digital data.
- 8 What device is usually used to connect a home network to the Internet?
A modem
- 9 What is one limitation of wireless technology in a home environment?
Limited available bandwidth for some applications, subject to interference
- 10 What is one advantage of wireless technology in a DHTI system installed in an older home?
No new wiring required, less expensive
- 11 What is HVAC?
Heating, ventilation, and air conditioning
- 12 How can DHTI reduce home utility costs?
It can reduce resource use when not needed and use resources during off peak times for maximum economy.
- 13 What does a satellite television hookup require for each television set connected to it?
A decoder to render the received signal into viewable form.
- 14 Why is a central DHTI processor usually better than independent processors in subsystems?
It permits the greatest degree of integration of DHTI subsystems, prevents conflicts between systems, and promotes maximum efficiency.
- 15 When installing infrastructure wiring, why is it usually better to install more than just the required capacity?
Technology is continually growing and the need for additional future capacity is almost ensured.
- 16 All of the following can be detected by a sensor except:
- A Heat
 - B Smoke
 - C Time**
 - D Motion
 - E Pressure

17 What is a firewall in a computer system?

A hardware or software device that controls the data entering or leaving the system to provide security

18 Can a computer virus reside in a sensor?

No, a sensor can only detect activity or conditions; it has no capacity to contain a virus.

19 If the outside temperature dropped suddenly to freezing, what actions might a complete DHTI system take in response?

It can shut off the outside water system, activate the de-icing system, and adjust the HVAC system.

20 You work for High Tech Home Tech, Inc. as a DHTI system designer and installer. A client calls you and requests information on what DHTI can do for her home environment. She tells you that she lives in an apartment on the fourth floor that is accessed by elevator and stairway. The home has two entrances, but she must use the elevator because she uses a wheelchair for mobility. She has full use of her hands and upper body and has no sensory limitations. She prefers to live alone, but wants to have some additional safety and security as well as convenience added to her home. Write a brief report summarizing what DHTI can do for this client's lifestyle. Divide your recommendations into categories that include safety devices, security devices, convenience devices, and entertainment systems.

A thorough answer might include that you could configure the home to automate opening doors, adjust temperature and lights, and control window coverings, security, and entertainment systems from a central control device.

Unit 2

Computer networking

Unit time: 210 minutes

Complete this unit, and you'll know how to:

- A** Configure a LAN connection.
- B** Share resources on a network.
- C** Create an Internet connection.
- D** Implement network protection strategies.

Topic A: Networking configuration

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
1.1	Identify basic networking protocols and their uses and know when/how to apply them. <ul style="list-style-type: none">• DHCP• UDP• DNS• TCP/IP• Subnet masks
1.3	Configure setup and maintain a residential LAN (Local Area Network). <ul style="list-style-type: none">• Client configuration<ul style="list-style-type: none">• Resource sharing• Peer-to-peer• Network device setup and integration<ul style="list-style-type: none">• Routers• Hubs• Switches• PoE (Power over Ethernet)
1.4	Configure setup and maintain a secure wireless network. <ul style="list-style-type: none">• Differentiate applications of hardwired vs. wireless networks
1.5	Identify and define network cabling characteristics and performance. <ul style="list-style-type: none">• Cable types<ul style="list-style-type: none">• Cat5• Cat5e• Cat6• Fiber• Coax• Cable length limitations• Protocols<ul style="list-style-type: none">• 10BaseT• 100BaseT• 1000BaseT• Shielded (STP) vs. unshielded (UTP)

Network types

Explanation

There are two basic types of networks that a CEA-CompTIA DHTI+ technician will encounter:

- **Peer-to-peer network** — This type of network, as illustrated in Exhibit 2-1, usually consists of several client computers that are connected to a network for simple file and printer sharing in a small office or home office. Each computer has a network card, which is connected to the network by a network cable or a wireless network card. All the communication is among the client computers. There are often fewer than a dozen users and computers. When accessing one computer from another, you must have an account on the computer you want to access.

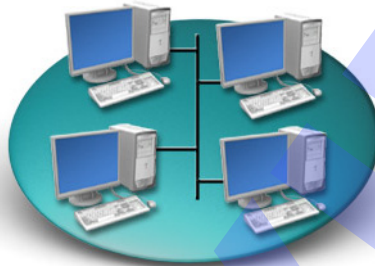


Exhibit 2-1: A peer-to-peer network

- **Client/server network** — In this type of network, as illustrated in Exhibit 2-2, computers called *servers* hold data and provide a wealth of services that users can share. Most of the communication is between the client computers and the servers. Client/server networks usually have at least one server with a central database of user accounts that are used to authenticate users. (In Windows, this server is called a *domain controller*.) On this type of network, users can log on and use whatever resources their user accounts allow them to use without needing an account for each computer. (Networks without a domain controller require separate user accounts for each computer; such a setup isn't easy to manage or maintain). There are often dozens, hundreds, or thousands of users. Such a network can span a building, an office park, a country, or the globe. Client computers are connected to the network via network card and network cable or a wireless connection.

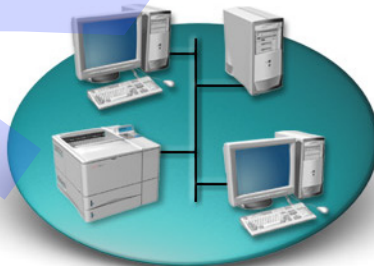


Exhibit 2-2: A client/server network

Network operating systems

A *network operating system (NOS)* manages local area network (LAN) resources. Windows 2000 is a series of operating systems, each designed for a particular size computer and computing needs. Windows 2000 Server is a network operating system, while Windows 2000 Professional is appropriate as a client operating system, just as Windows XP Professional is.

Windows Server 2003 comes in many editions, each designed to meet certain needs with specific system requirements. Both the Standard and Enterprise Editions of Windows Server 2003 come with a built-in firewall. The four Windows Server 2003 operating systems editions are:

- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Windows Server 2003, Web Edition

A Windows 2000 Server or Windows Server 2003 domain uses one or more domain controllers that replicate the database among themselves. In other words, the database is stored on all domain controllers instead of on only one. This type of configuration is useful for organizations that need to keep things running in the event of a domain controller failure. Users might be unaware of a domain controller failure because they can still continue using their computers and network resources. Windows 2000 Server and Windows Server 2003 keep lists of network resources in a database called Active Directory.

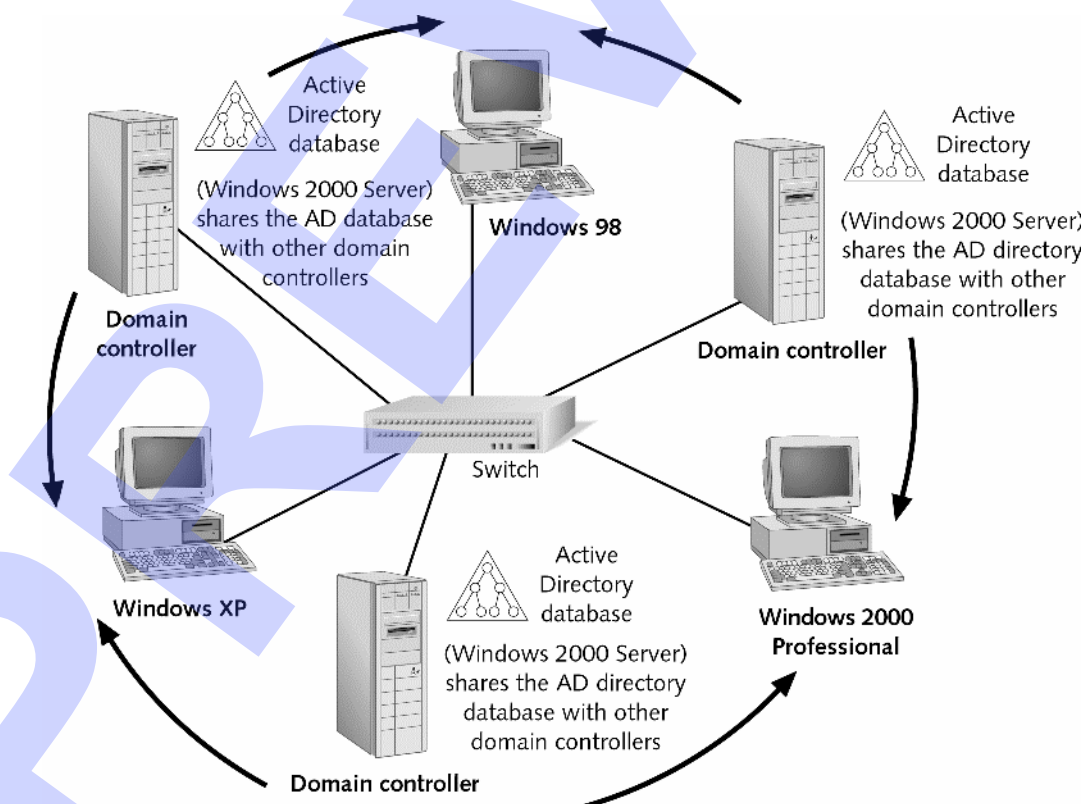


Exhibit 2-3: A Windows 2000 Server domain



Active Directory is a centralized system that controls computer and user configuration settings, security settings, and access to resources on a LAN. It uses a hierarchical organization that provides the administrator with a single place for all system administration, including user and computer configuration and management. Active Directory follows the client/server model and allows users to access network resources from any computer on the network. The Windows 2000 Server Active Directory management console GUI is nearly identical to the one found in Windows Server 2003, but it lacks some management features and tools.



UNIX and Linux

Until recently, UNIX was the only reliable option for an NOS that provided services over the Internet. TCP/IP was born in a UNIX environment. UNIX also can support a LAN as a file and database server, managing user accounts and access privileges. UNIX was also the first, and still is the most popular, NOS for midsize servers responsible for supporting thin clients. Java was developed in a UNIX environment to support thin clients served by a UNIX computer. The first Web servers used UNIX. It's also the accepted mainstay for the firewall market.

UNIX isn't an easy operating system to learn. Even though it does offer a GUI interface, a system administrator can't fully perform his or her job without a working knowledge of a somewhat cryptic command-line shell. Installing UNIX and installing hardware devices on a UNIX system require expertise far beyond that of a casual user.

Linux is quickly becoming a viable option as a NOS. Red Hat, Inc. (www.redhat.com) sells an impressive version of Linux that has proven to be competitive as an NOS for Internet services.



Network services

For smooth operations and ease of manageability on client/server networks, servers provide a variety of network services. These services enable users to share files, communicate with one another via e-mail, share printers, compile information in centralized databases, and access the Internet. The following table describes some important network services.

Service	Description
Dynamic Host Configuration Protocol (DHCP)	DHCP assigns numerical addresses to computers in the network. These addresses, called <i>IP addresses</i> , are used to identify each computer uniquely and are needed for computers to communicate on the network using TCP/IP. This network service is hosted on a server called a <i>DHCP server</i> . Administrators use DHCP so they don't have to manage address assignments manually, which can get complicated on networks with thousands of computers.
Domain Name Service (DNS)	DNS translates computer names, called host names or <i>DNS names</i> , into IP addresses on a LAN and on the Internet. DNS servers maintain a database that contains name-to-address mappings. It's DNS that enables you to enter "www.yahoo.com" instead of having to remember a numerical address such as 216.109.118.75. The process of translating a familiar name into an IP address is called <i>name resolution</i> .
Windows Internet Naming Service (WINS)	WINS is similar to DNS, but it translates IP addresses into simpler computer names, such as "Computer100," which are called NetBIOS names. WINS was widely used in earlier Microsoft networks, but with Windows 2000, Microsoft came to rely more on DNS, because DNS provides more flexibility in naming computers in large networks.
Authentication	Servers that provide authentication services are used to restrict access to the network and other computers and the services they offer. In Windows networking, servers that provide authentication are called <i>domain controllers</i> . Windows domain controllers run Windows NT Server 4.0, Windows 2000 Server, or Windows Server 2003.
Internet access	Some servers act as a gateway between an organization's private LAN and the Internet, funneling communication between computers on the network and those on the Internet. Some servers and devices protect the network from malicious activity on the Internet; these are called <i>firewalls</i> .
File sharing	Some servers just store files or databases that are accessed by network users. These servers' only function is to hold data and make it available to users across the network.
Printing	Printers can be connected to the network if they have networking capability and a network card built in. Printers without that capability must be connected to a computer that offers the printer's services to network users.

Client operating systems



On a LAN, each personal computer must have an operating system that's capable of interfacing with a *network interface card (NIC)*, also called a *network adapter*, and the resources available on the network. A NIC is the hardware device inside a computer that works with the client OS to provide access to a network. Personal computer OS options include all Windows XP versions, Windows 2000 Professional, Windows NT Workstation, Windows 98, Mac OS, and Linux, which can all function as client operating systems.

Windows 9x and Windows Me



Explain to students that the 9x designation is used to refer to the Windows 95 and Windows 98 family of operating systems together.

Microsoft ended support for Windows 98 and Windows Me in June 2006.

Windows 95, *Windows 98*, and *Windows Me* are older client operating systems that are still used on many home computers. Windows 9x is backwards compatible with MS-DOS, Windows 3.x, and older (legacy) hardware devices. Some devices that are found on newer computers might not function correctly under Windows 9x. You can look at the speed and configuration of a computer to decide whether to install Windows 9x or Windows Me. Slower systems such as an Intel Pentium II 350 MHz would run Windows 9x perfectly.

Windows 9x and Windows Me support network access and can be used in a peer-to-peer or client/server network. Using the OSs, you can give others on the network access to files and folders on your hard drive (or even the entire hard drive) and to a printer that's directly connected to your computer. For this feature, file and printer sharing must be installed and individual files, folders, and printers must be shared. Windows 9x users on a LAN might not be able to access shared resources, such as files on Windows 2000 or Windows XP computers. This can happen if Windows 2000 or Windows XP computers are configured to use NTFS. NTFS is a newer technology that is used to manage files and folders on a hard drive. It offers greater stability and security than older file systems used in Windows 9x and Windows Me.

Windows NT Workstation, Windows 2000 Professional, and Windows XP



Microsoft has sold many client operating systems over the years. One of the oldest that's still in use is Windows NT. It offers two operating systems, *Windows NT Workstation* and *Windows NT Server*. By the late 1990s, Windows NT Workstation was widely used by many small and large businesses. It worked well in a peer-to-peer network or in a client/server network.

However, by today's standards, Windows NT Workstation is often difficult to set up and to configure device drivers because Windows NT Workstation doesn't use the Device Manager graphical user interface. Windows NT Workstation also lacks plug-and-play capabilities. Plug-and-play is used to install drivers automatically for new devices that are added to a computer. Occasional computer problems were common as software vendors struggled for many years to write stable programs for Windows NT Workstation.

Microsoft ended its support for its Windows NT product line in January 2005. However, many businesses had already upgraded their Windows NT Workstation computers to Windows 2000 Professional.

The Windows 2000 OS family has four different operating systems, depending on your needs: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server. Of these four, Windows 2000 Professional is appropriate for use as a client OS. Windows 2000 Professional was based on the technology used in Windows NT but offers better support for devices than Windows NT. It's more reliable than Windows NT Workstation and offers a user-friendly interface. Some businesses have already upgraded their computers to Windows XP, although others still use Windows 2000 Professional.

In this text, the term Windows XP refers to Windows XP Professional.

Windows XP comes in four different operating systems: *Windows XP Professional*, *Windows XP Home Edition*, *Windows XP Media Center*, and *Windows XP 64-Bit Edition*. Windows XP is very similar to Windows 2000 Professional but offers much wider support for devices, such as printers, NICs, USB devices, and others. The Windows XP default Start menu is very different from any previous Microsoft operating system and offers instant access to frequently used programs. Windows XP also offers a Classic View Start menu that's nearly identical to the one found in Windows 2000 Professional. Windows XP Home Edition and Media Center have a user interface that's identical to Windows XP Professional, but that lacks some networking features found in Windows XP Professional. As its name implies, Windows XP Home Edition is meant for home users. Windows XP Home Edition and Media Center computers can't be used on a client/server network where the NOS is Windows Server 2003, Windows 2000 Server, or Windows NT Server. However, Windows Home Edition and Media Center are useful on small, peer-to-peer networks. Windows XP Home Edition and Media Center are designed to replace Windows 9x, Windows Me, Windows NT Workstation, and Windows 2000 Professional that still exist in many homes and small offices. Windows XP Professional is designed to replace older operating systems used in medium to large offices. Windows 64-Bit Edition is similar to Windows XP but has been optimized for newer, 64-bit processors. It's intended for people who use highly technical software applications.

When considering whether to use Windows 2000 Professional or a Windows XP version on a computer, verify that all the hardware and software already installed on the computer is compatible with the new operating system. For hardware, check the Hardware Compatibility List (HCL) on the Microsoft Web site, www.microsoft.com/hcl. If your specific hardware isn't listed, you most likely can't successfully install Windows 2000 Professional or Windows XP on the system without contacting the hardware manufacturer directly for updated drivers.

Linux

There was a time when UNIX wasn't considered a viable option as a personal computer OS, but that changed in 1991 when Linux was invented. Linus Torvalds created Linux with the help of volunteers from all over the world. Linux was designed as a scaled-down version of UNIX. It's free, although companies offering Linux charge a price for the documentation, technical support, and add-on modules. Linux is small enough to fit and run on a computer that's 10 years old, yet it has network capabilities similar to a full-fledged commercial version of UNIX. For a time, Linux was considered only a training tool for learning UNIX, because it could be installed on an inexpensive, low-end computer and easily used in a training environment or at home. Linux is no longer considered just a training tool and is rapidly gaining acceptance as an operating system of choice in certain situations.

Remind students that a proxy server is software that acts as the intermediary between the Internet and other computers on the network.

Linux is an excellent NOS to use in a small company environment with low-volume traffic for intranet services. It can be used as the OS for a Web server or proxy server for a LAN. Apache Web Server, a popular Web server application, is often used on a UNIX or Linux platform. Even though Linux generally isn't considered an appropriate OS for the kind of high-volume traffic that UNIX is known to handle, several high-traffic Web sites now run successfully using Apache Web Server on a Linux platform. As a result, the industry's perception of Linux is quickly changing.

Linux's popularity is also growing. Apple, Computer Associates, Compaq, Corel, Dell, Hewlett-Packard, IBM, Informix, Intel, Lotus, NAI, Netscape, Novell, Oracle, SAP, and Sybase are among the companies that have recently provided support for their products using the Linux OS. The largest drawbacks to using Linux in a corporate environment don't so much entail the technical strength of the OS but the support and standards surrounding it, the lack of application software written for it, and the lack of experienced technical support people.

Linux is very different from Windows. To evaluate Linux as an operating system, you need to understand the difference between an operating system kernel and an operating system shell. The operating system kernel is the part of the operating system that interfaces with the hardware (including the NIC) that accesses the network. The user or applications software can't command the kernel directly but must go through a command interface called the shell. Applications software must also interface (communicate) with the OS through the shell and, in most cases, can't access the hardware directly. The Linux kernel is considered a much more stable operating system kernel than the Windows kernel, which results in fewer Linux crashes than Windows crashes in comparable situations.

Linux and UNIX use a command-line shell as the default shell. On newer versions of Red Hat Linux, the user can load a GUI shell similar to the Windows user interface. Linux isn't as popular an operating system for personal computers as Windows. It can be difficult to install, because the software responsible for communicating with Linux to interface hardware devices (called drivers) isn't as readily available for Linux as it is for Windows, and the installation can sometimes be very complex. Even so, many applications are being written for Linux, and GUI shells are becoming standard.

Macintosh operating system

Several versions of the Macintosh operating system (Mac OS) are available for Macintosh computers, the latest being Mac OS X (10). OS X provides easy access to the Internet and allows any Macintosh computer to become a Web server for a small network. The Mac OS has an excellent icon-driven interface, and it's easy to learn and use. Many applications exist for the Mac OS to create and edit graphics, build Web sites, and manage multimedia devices.

The Mac OS uses a suite of networking protocols called *AppleTalk* but also supports the networking protocol suite TCP/IP. Thus, it can access the Internet and other TCP/IP networks. Mac OS X supports TCP/IP networking out of the box and can communicate with Windows computers on any TCP/IP network.

Do it!

A-1: Discussing network models

Questions	Answers
1 How are client/server networks different from peer-to-peer networks?	<i>Client/server networks have servers in addition to client computers. Client/server networks are also usually larger and offer more services than peer-to-peer networks.</i>
2 Why would a company want to implement a client/server network?	<i>A company would implement a client/server network if it has resources (files, printers, databases, Internet access) it wants to share among a large number of employees.</i>
3 What kind of company would implement a peer-to-peer network?	<i>A small company that wanted to share files or a printer among a small number of client computers.</i>

Network interface card (NIC)

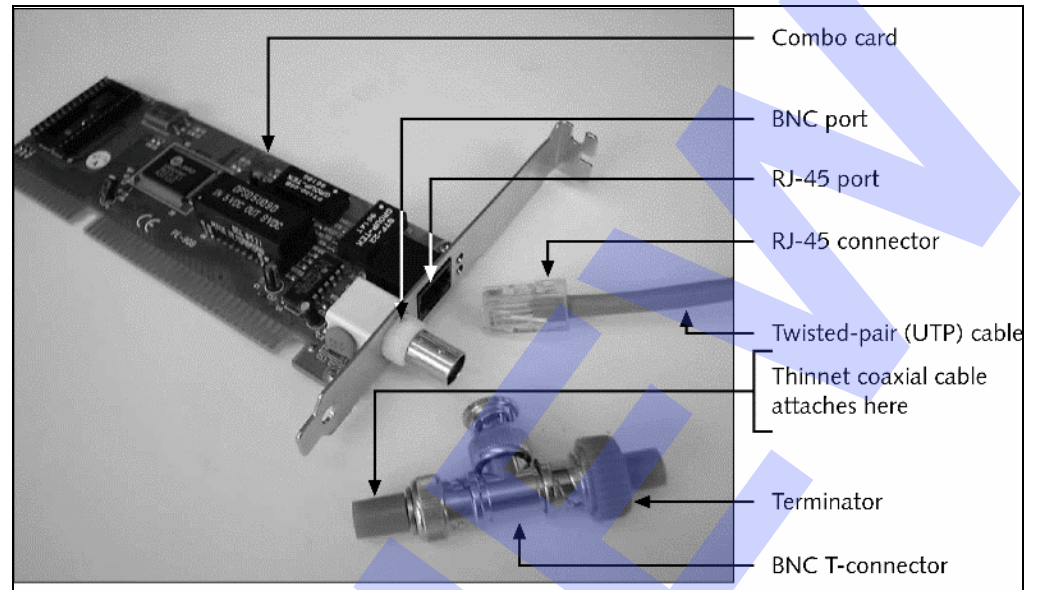
Explanation



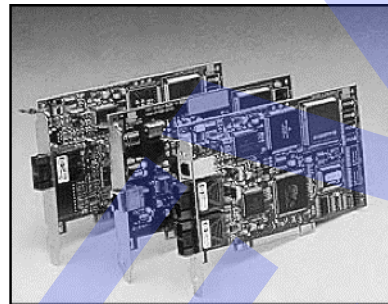
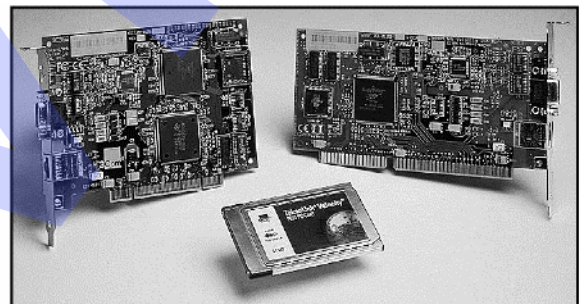
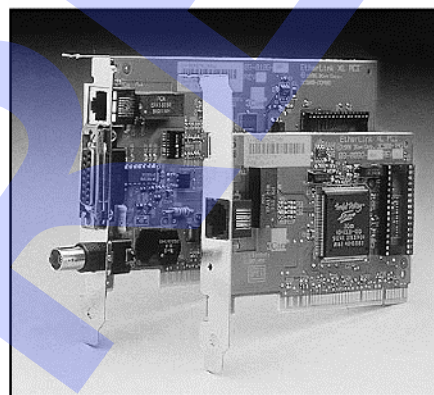
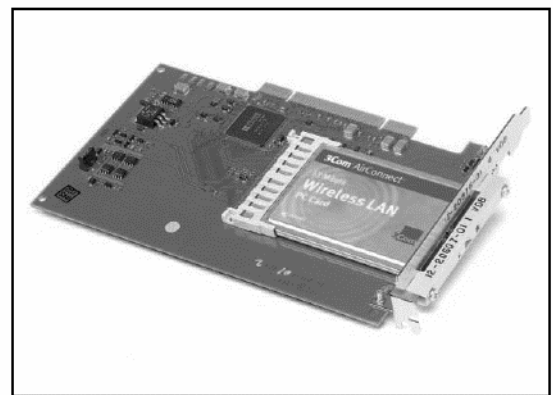
A network interface card (NIC) is an adapter card that plugs into one of the expansion slots that all PCs have on their motherboards, or it attaches to the computer through an external port, such as a USB 2.0 port. The NIC has one or more ports built into it that are used to connect the NIC and its computer to a network using a cable that plugs into the port or wireless radio waves. A NIC can support Ethernet, token ring, or FDDI network architecture, but only one of the three. It may have ports that can accept more than one type of cable connection. For example, an Ethernet card might have connectors for both coax and twisted-pair with a BNC connector and/or DB-15 DIX connector for coax cables and an RJ-45 connector for twisted-pair cables.

The function of the NIC is to send and receive information from the system bus in parallel and to send and receive information from the network in series. The NIC also converts the data that it receives from the system into a signal that's appropriate to the network. For an Ethernet card, this means converting the data from the 5-volt signal used on the computer's motherboard into the voltage used by twisted-pair cables. The component on the NIC that makes this conversion is a transceiver. An Ethernet card may have more than one transceiver to convert data into the appropriate voltage for various types of cable connectors, which are wired into the NIC. Such cards are called combo cards. A combo card is shown in Exhibit 2-4. Exhibit 2-5 shows other examples of NICs.

D

*Exhibit 2-4: An Ethernet combo NIC*

D

**a. FDDI****b. Token Ring****c. Ethernet****d. Wireless***Exhibit 2-5: Examples of network interface cards (NICs)*



NICs have built-in identifying addresses coded into them by the manufacturers. These codes are used by the network to identify the computer (node) using the card. These addresses are called *media access control (MAC) addresses*, physical or adapter addresses, or Ethernet addresses. They consist of 6-byte (48-bit) hexadecimal codes, which are unique for each card. Part of the address contains the manufacturer identifier, and the rest is a unique number. No two NICs have the same identifying code.

When selecting a NIC, it's critical to match it with the network architecture to which it connects, the specific type of cable connection it uses, and the type of slot in the computer (PCI or ISA) in which it's installed.

All internal cards for desktop systems are PCI cards at this point. If you're supporting older equipment, you might encounter some ISA or EISA cards in which you need to configure the IRA, DMA, and I/O addresses. A utility from the manufacturer is used to configure the settings on such cards.

Some network adapters are also available in USB versions to connect externally without the need to open the case. This is usually available for wireless rather than wired network adapters.

Do it!

A-2: Installing a wireless network adapter

If the NIC plugs into a USB port, have students install it by referring to the documentation that came with the USB device.

Here's how	Here's why
1 Shut down the computer	You will add a wireless network adapter to your system.
Unplug the computer from its power source	Many components, including network cards continue to receive power even if the computer isn't turned on, so it's best practice to unplug the computer in addition to turning it off.
2 Remove the case	To access the slots on the motherboard.
3 Install the NIC into the slot	Be sure it's fully seated into the slot.
Attach the NIC to the case	If there's no screw, just be sure that the card is fully seated in the slot.
4 Replace the case	
5 Plug the computer into the power source	
6 Turn on the computer	
7 If prompted to install drivers, follow the prompts to do so	

Hardwired and wireless networks

Explanation

The home network can be a hardwired system, wireless, or a combination of both, but it must provide a far greater degree of compatibility and adaptability to individual components and systems operating on different protocols and standards than is usually required in business systems.

Home technology systems are usually engineered to give adequate performance in specific consumer applications at minimum cost. This design standard makes such systems affordable for the average homeowner, but often requires some limitations in the hardware, protocols, or other design parameters as compared to business-oriented networks.

Exhibit 2-6 shows a home network with both wired and wireless segments.

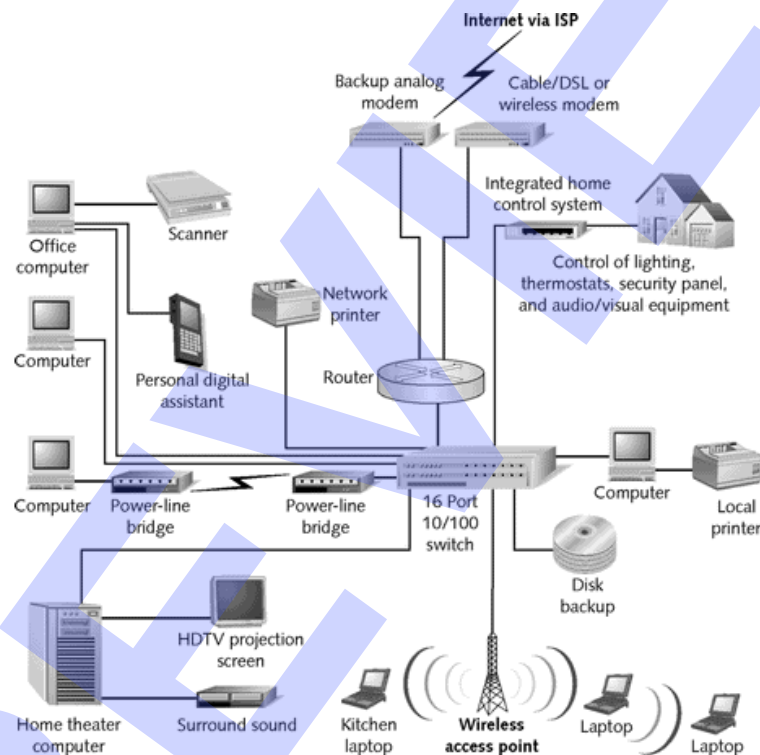


Exhibit 2-6: A home LAN may have wired and wireless segments

Hardwired networks are not as susceptible to having data intercepted by unauthorized persons as wireless networks are. While you can take certain measures to help secure a wireless network, a hardwired network is much more secure than a wireless network.

If you want anyone and everyone to have access to the network, a wireless network is a great solution. This is the type of network used in public places that provide WiFi access to customers.

Do it!

A-3: Discussing when to use hardwired vs. wireless networks

Questions and answers

- 1 You are installing a network in a historic home. The owners are reluctant to drill any holes in floors, walls, or ceilings. They would like to have computers in the family room, the home office, and the master suite. They also are concerned about the security of the network, especially for the work done on the home office computer. Describe the network you would recommend for this home.

A wireless router with wired ports should meet the needs for this network. The Internet connection could be run to the home office, and the router could reside there, with a hardwired connection for the PC in the office. The computers in the family room and master suite could then use wireless connections to access the network and the Internet.

- 2 You have been hired to install a network at a coffee house. The owner would like to offer free Internet access to the customers. She would like the access for customers to be as easy as possible so that the baristas do not have to answer questions about network access for customers.

A wireless network with open access would be the best solution for this particular customer.

- 3 A home business owner has contacted you to configure a new network in his office. He is an accountant that does financial planning and tax preparation for his customers. He works from a basement office that adjoins the family room where the cable TV connection is located.

A wired network should be used in this case if possible since it is more secure than a wireless network.

Wiring an Ethernet network

Ethernet is the type of network that is almost always used in home networks. Ethernet networks use UTP or STP wiring for all the connections in the network. They can use coaxial cable or even fiber optic cable, but both of these are more expensive than UTP or STP cable and also use more costly plugs and jacks or other connectors, which further increases their cost differential. The vast majority of home LANs using Ethernet topology are wired a version of UTP called Category 5 cable. Category 5, 5e, or even 6 are other options of higher capacity, more secure UTP cabling that can be used. Exhibit 1-1 shows the composition of UTP and STP cable as well as that of coaxial cable and fiber optic cable.

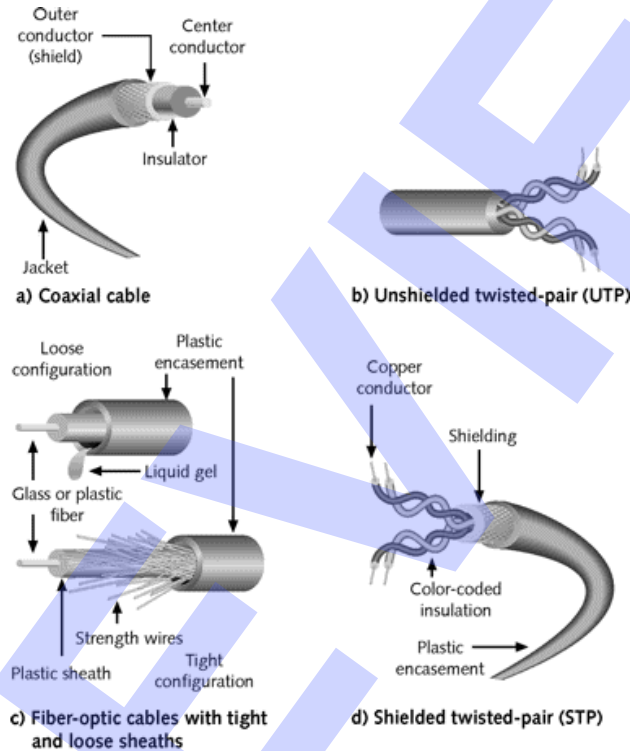


Exhibit 2-7: Networking cables

The following table compares how the different cables are used in the various Ethernet configurations and the maximum length the cables can extend.



Cable system	Speed	Cables and connectors	Max. cable length
10Base2 (ThinNet)	10 Mbps	Coaxial uses a BNC connector	185 meters or 607 feet
10Base5 (ThickNet)	10 Mbps	Coaxial uses an AUI 15-pin D-shaped connector	500 meters or 1,640 feet
10BaseT and 100BaseT (twisted-pair)	10 to 100 Mbps	UTP or STP uses an RJ-45 connector	100 meters or 328 feet
1000BaseT	1000 Mbps	UTP or STP uses an RJ-45 connector	1000 meters
10BaseF, 10BaseFL, 100BaseFL, 100BaseFX, or 1000BaseFX (fiber optic)	10 Mbps up to 1 Gbps	Fiber optic cable uses an ST or SC fiber optic connector	500 meters up to 2 kilometers (6,562 feet)

In many newer homes, UTP or STP wiring is installed during construction so that every room in the home is wired for network service in much the same manner as it is wired for electrical service. The contractor rarely installs the network equipment, but simply puts the wiring in place, adds standard connectors, and finishes the connecting point boxes in the walls with cover plates. When the homeowner is ready to install a network, he or she can refer to the wiring diagram provided by the contractor and connect the network components directly into the wall-mounted points without the need to install any wiring except the patch cables from the wall connectors to the nodes.

If a home has installed UTP or STP wiring, it's definitely the best option to use for a network. All the other wired and wireless network technologies have some potential drawbacks (limited capacity, potential for interference, slower speeds, and so on) that make them poorer choices for network infrastructure even under ideal conditions.

Most home LANs, however, aren't installed under ideal conditions. Network wiring as a built-in feature has been around only for a few years, and not all the homes constructed even during the last decade have it. It is estimated that less than five percent of current U.S. homes have UTP or STP wiring put in at the time of construction. For all the rest, installation of wiring after the home is completed is more difficult and more expensive. For many of them, other alternatives may be preferable.

In existing homes, network wiring must be installed by running or pulling it through the walls from access opening to access opening in order to provide connecting points in all the rooms where network service is desired. Pulling wires through existing walls often means taking the easiest route for running the wires, rather than the shortest. This tends to increase the amount of cable used over the amount used in a comparable new home where the wiring can be run more economically via the shortest routes.

Pulling wire for an installation in an existing home nearly always uses more wire, takes more time, and does some damage to the home (holes in the walls, moldings removed, and so on) that must be repaired. As a general rule, the older the home is and the more often it has been renovated in the past, the more difficult and expensive it is to wire it for a network.

Heavy construction (brick, concrete block, plaster over wood lath, or heavy wall board) is more difficult to work with than lighter construction (wood siding, stucco, or plasterboard interior walls).

As you consider whether to install new wiring for a home LAN, carefully evaluate how long the job will take and how much damage will require repairing. Substantial homes built before the 1960s may well be exceedingly difficult to retrofit with new wiring. And some built before the 1930s may be virtually impossible without literally destroying a substantial part of the structure.

As the potential cost and difficulty of retrofit wiring increase, the use of other wired or wireless technologies for a home network becomes more attractive. Several of these technologies are less expensive to begin with than dedicated network wiring. If the cost differential mounts in a particular application, it won't be difficult for the network designer to see that another choice of technology is best for the job.

Routers, hubs, and switches

Routers are the hardware units responsible for directing data traffic between interconnected networks. They function as intelligent switches that have the ability to make decisions based on preprogrammed instructions and implement those decisions by directing electronic data along specific routes. They read the IP addresses of each packet of data that comes to them, decide which is the most efficient path for the data to take to reach its destination quickly, and then switch the data packet onto that path.

A switch is similar to a router. Using the MAC address, it determines which port the data should be sent to and sends the data only to that particular port.

A hub connects nodes within the LAN. It broadcasts data received from any node to all other nodes.

Power over Ethernet

Power over Ethernet (PoE) is a network technology that supplies both power and data over a single Cat5 Ethernet cable. It is also known as IEEE 802.3af. This is done by using a Cat5 Injector, which adds DC voltage to the cable. The Injector usually is added near the Ethernet hub or switch. This technology provides VoIP phones, Web cameras, point-of-sale terminals, wireless access points, and other LAN devices power and the ability to send and receive data using existing network Ethernet infrastructure rather than needing to place devices where they have access to an electrical outlet for its power supply. An example of a PoE installation is shown in Exhibit 2-8

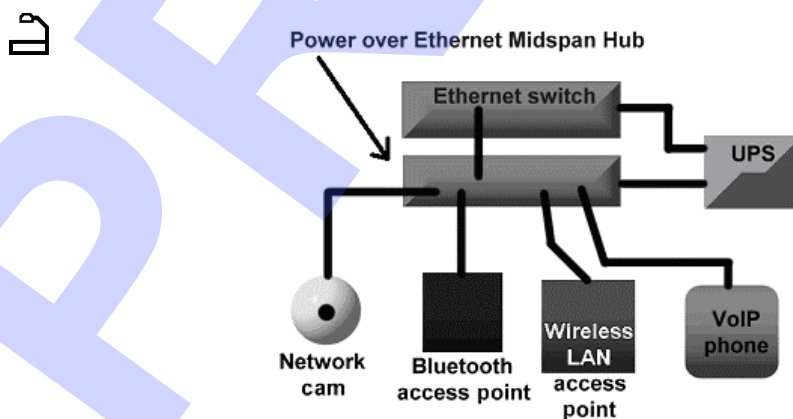


Exhibit 2-8: A PoE installation.

Do it!

A-4: Identifying characteristics of wired cable types

Questions and answers

1 Most Ethernet networks use which type of cable?

Category 5 UTP cables

2 What is the main difference between UTP and STP cable?

UTP contains no shielding material.

3 Which Ethernet cable reaches the furthest?

Fiber optic

4 Why are older homes typically more difficult to retrofit with UTP cabling?

They used heavier construction materials such as brick, concrete block, plaster over lath, or heavy wall board.

5 Which takes more wire, wiring new construction or retrofitting old construction?

Old construction

Network protocols

Explanation



In addition to one or more operating systems, a network also requires a network protocol, so all computers on the network can communicate. Network *protocols* are the languages that computers, servers, and network devices use to communicate with each other. Protocols send data across the network in units called *packets*. To communicate, all computers, including the NOS on the server, must use the same network protocol. The selected network protocol must be supported by every operating system on the network. The following table lists some common network protocols that you can use in Windows networks.



Protocol	Description
Transmission Control Protocol/Internet Protocol (TCP/IP)	A routable, nonproprietary protocol that's the predominant Windows network protocol. It's supported by all versions of Windows and most other non-Microsoft operating systems. TCP/IP is also the protocol of the Internet.
User Datagram Protocol (UDP)	A protocol that can be used in place of TCP when transporting simple messages that are a single packet in length. This protocol doesn't acknowledge receipt of packets.
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)	A routable, proprietary protocol that was the native protocol in early versions of Novell NetWare. Later versions of NetWare supported TCP/IP as the native protocol. Windows computers can connect to IPX/SPX networks and NetWare servers by using Microsoft's version of IPX/SPX, called NWLink. To share files and printers on a NetWare server, you must install the Microsoft Client for NetWare.
AppleTalk	<p>A routable network protocol supported by Apple Macintosh computers. Windows NT and Windows 2000 support AppleTalk. Mac OS X (10.2 and later) supports TCP/IP and can connect to Windows networks without requiring AppleTalk support.</p> <p>AppleTalk computers are called <i>nodes</i> and can be configured as part of <i>zones</i> for sharing resources. Each node on a network must be configured with a unique network address.</p>
NetBEUI	<p>A nonroutable, proprietary Microsoft protocol that's supported in Windows 9x/Me, Windows NT, and Windows 2000. NetBEUI uses Network Basic Input/Output System (NetBIOS) services to communicate with other computers on a network. (NetBIOS helps with computer names and some basic communication services.) Although it isn't technically supported in Windows XP, you can install NetBEUI by manually copying files from the installation CD-ROM.</p> <p>What's nice about NetBEUI is that it has no settings to configure. You install the protocol, connect the computer to the network, and it just works. The drawback is that it isn't routable, so it can't pass from one network segment to another. This means it can't be used for remote access or any communication outside a single segment.</p>

To view the network protocols that are supported by Windows XP:

- 1 Click Start and choose Control Panel.
- 2 In Category View, click Network and Internet Connections.
- 3 Click Network Connections. The network devices installed on your computer are listed. If a NIC is installed, you see a Local Area Connection icon.
- 4 Right-click the Local Area Connection icon and choose Properties.
- 5 Click Install.
- 6 Select Protocol and click Add. The Select Network Protocol displays the three network protocols supported by Windows XP: Microsoft TCP/IP version 6; Network Monitor Driver, and NWLink IPX/SPX/NetBIOS Compatible Transport Protocol.
- 7 Click Cancel three times.

TCP/IP provides the LAN with access to the Internet. Sometimes, however, a network must support more than one network protocol, because each protocol is used for a different purpose. For example, if the NOS on the server is Novell NetWare 5.0 or below, the client computer must have the NWLink IPX/SPX/NetBIOS Compatible Transport protocol installed. Installing this protocol in Windows XP actually installs the IPX/SPX protocol and the NetBIOS protocol. The IPX/SPX protocol is used to route and check data for errors. The NetBIOS protocol allows one application to communicate with another application on the same LAN. It isn't unusual for computers on a LAN to use several different protocols, each for a different purpose.

Do it!

A-5: Viewing installed network protocols

Here's how	Here's why
<ol style="list-style-type: none"> 1 Click Start, and choose Control Panel 2 Click Network and Internet Connections Click Network Connections Right-click Local Area Connection, and choose Properties 3 Click Cancel Close the Network Connections window 	<div> <p>This connection uses the following items:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Client for Microsoft Networks <input checked="" type="checkbox"/> File and Printer Sharing for Microsoft Networks <input checked="" type="checkbox"/> QoS Packet Scheduler <input checked="" type="checkbox"/> Internet Protocol (TCP/IP) </div> <p>TCP/IP is the only protocol installed on the computer for network communication.</p>

If students are using a wireless connection, right-click Wireless Network Connection

TCP/IP configuration

Explanation

TCP/IP is the network protocol in just about every organization, so it's important to know how to configure TCP/IP on client computers. Basic TCP/IP configuration consists of the IP address and subnet mask, examples of which are shown in Exhibit 2-9.



Use the following IP address:

IP address: 192 . 168 . 100 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

Exhibit 2-9: IP address and subnet mask

IP addresses



Each computer on a TCP/IP network is assigned a unique numerical address called an IP address. An IP address is like a house number or a cell phone number. It's used to provide a unique identification that distinguishes the computer it's assigned to from all other computers. Without an IP address, a computer can't communicate on a network using TCP/IP.

IP addresses consist of four one-, two-, or three-digit numbers separated by periods, like this: 192.168.115.231. You must have all four parts of the number for the IP address to be complete. Part of the IP address defines the network address, also known as the *subnet*; the other part of the IP address defines the computer address. Taken together, the two parts uniquely identify a computer, much like an area code and phone number identify a specific phone. In the example 192.168.115.231, the network portion of the address (the area code) is 192.168.115, and the computer address (the phone number) is 231.

IP addresses can be assigned manually in the Windows GUI, or they can be assigned automatically by DHCP. When you assign an IP address manually, you enter it in a dialog box. A manually assigned IP address is called a *static IP address*.

When you use DHCP, you tell the computer to ask the DHCP server for an address. The DHCP server sends the address to the computer and keeps track of all addresses it has assigned to all computers, so there are no conflicts. The computer then uses that address as its IP address.

Windows 2000 and Windows XP computers can assign themselves IP addresses by using *Automatic Private IP Addressing* (APIPA). They assign themselves IP addresses in the range of 169.254.0.0 to 169.254.255.255, if they haven't been assigned an IP address manually, and there's no DHCP server on the network. APIPA is a great feature for a small network, because the computers just assign themselves IP addresses, and you don't have to worry about doing it manually or setting up a DHCP server.

Subnet masks

The *subnet mask* is a number that looks something like an IP address. Its function is to separate the IP address into the network address and the computer address so that routers and other network devices know where to send data packets. A subnet mask often looks like this: 255.255.255.0. This example would be the default subnet mask for the IP address example in the preceding section; this subnet mask would tell other computers and routers that 192.168.115 is the network address and 231 is the computer address.

Subnet masks can get very complicated, but as a CEA-CompTIA DHTI+ technician, you don't have to worry about figuring them out. You just need to assign the appropriate subnet masks, which the network administrator or engineer provides, and you need to verify that a computer has been assigned the correct subnet mask if you're troubleshooting networking errors.

The DHCP process

If a computer is configured to use DHCP, when it starts up, it broadcasts a request across the network for a DHCP server. A DHCP server responds with an offer of an IP address and associated TCP/IP properties. The computer then uses this data to configure TCP/IP. If the computer can't get an IP address from a DHCP server, it has no IP address, or, if it's a Windows Me/2000/XP computer, it assigns itself an APIPA address.

The IP address is assigned or *leased* to the computer for a specified duration—anywhere from a few hours to a few days, depending on how the DHCP server is configured by the network administrator. If you need to update IP addressing information, you can remove the DHCP address that's been assigned to you and then manually send a request to the DHCP server for another IP address. This procedure, which you'll see later, is called *release and renew*.

IP address assignments

To assign an IP address or configure a computer to use DHCP:

- 1 In Windows 2000/XP, right-click My Network Places and choose Properties.
- 2 Right-click Local Area Connection and choose Properties.
- 3 Double-click Internet Protocol (TCP/IP).
- 4 Choose to use DHCP or assign an IP address manually.

Do it!

A-6: Configuring an IP address and subnet mask

Have a range of private IP addresses ready for students to use.

If students are using a wireless connection, they should right-click Wireless Network Connection.

Here's how	Here's why
<div>1 Click Start</div> <div>Right-click My Network Places and choose Properties</div>	<div>To open the Network Connections window. You're going to assign a static IP address.</div>
<div>2 Right-click Local Area Connection and choose Properties</div>	<div>To open the Local Area Connections Properties dialog box.</div>
<div>3 From the list of components, select Internet Protocol and then click Properties</div>	<div>To open the Internet Protocol (TCP/IP) Properties dialog box.</div>
<div>4 What's your current IP address?</div>	<div><i>It isn't displayed. Currently your computer has been assigned an IP address by a DHCP server.</i></div>
<div>5 Select Use the following IP address</div> <div>In the IP address box, enter the IP address supplied by your instructor</div>	<div><div><div>IP address:</div><div>192 . 168 . 100 . 185</div><div>Subnet mask:</div><div>. . .</div><div>Default gateway:</div><div>. . .</div></div><div>To assign a static IP address to your computer.</div></div>
<div>6 Press TAB</div>	<div><div><div>192 . 168 . 100 . 185</div><div>255 . 255 . 255 . 0</div></div><div>To enter a default subnet mask. You can change the subnet mask if necessary.</div><div>Leave the dialog box open for the next activity.</div></div>

Explanation



Additional TCP/IP properties

The following table lists some of the other TCP/IP properties you can configure. Keep in mind that these properties can also be assigned by using a DHCP server—a method that provides greater ease and flexibility when managing a large network.

Property	Description
Default gateway (gateway)	This is the IP address of the server on the subnet that forwards packets to other subnets. You need to configure a default gateway, if the computer needs to communicate with other subnets or with the Internet.
DNS server address	This is the IP address of the DNS server. The DNS server helps the client computer find other computers on the internal network or on the Internet. The DNS server might be on the LAN, or it might be maintained by the Internet service provider. There could be multiple DNS server addresses.
WINS server address	This is the IP address of the WINS server on the network. There could be multiple WINS server addresses. You see WINS used mostly in older Windows networks.

Computer names

All Windows computers have names. They can be simple and easy to remember, such as Computer1, or they can be more complex, such as cca-xp-89-444-00A.organization.int. Each organization determines its own computer naming scheme, with the understanding that computer names on the same network must be unique.

There are two types of computer names: NetBIOS names and DNS names. NetBIOS names look like this:

- Computer10
- Andy
- MyComputer
- Client1
- XPComp
- rco-313-00-A

DNS host names include a NetBIOS-type computer name plus the *DNS suffix* of the DNS domain of which the computer is a member. DNS host names typically look like this:

- computer10.class.internal
- support.microsoft.com
- www.course.com
- client100.local.mycompany.class

In these examples, the host names are computer10, support, www, and client100. The DNS suffixes are class.internal, microsoft.com, course.com, and local.mycompany.class.

You won't be responsible for creating names, but you might be responsible for assigning names and DNS suffixes to computers from a list you've been given. You might also find that computers with identical names on the same network are causing errors that prevent users from accessing the network. Understanding some naming basics is important.

Do it!

Be prepared with at least a default gateway and DNS server address. Provide other settings necessary for Internet access.

Be sure to use the DNS server configured on the classroom domain controller.

A-7: Configuring additional TCP/IP properties

Here's how

- 1 In the Internet Protocol (TCP/IP) Properties dialog box, press

TAB

Enter the default gateway supplied by your instructor

- 2 In the Preferred DNS server box, enter the IP address supplied by your instructor

- 3 Click **Advanced...**

- 4 Observe the IP Settings tab

- 5 Activate the DNS tab

- 6 Activate the WINS tab

- 7 Activate the Options tab

- 8 Click **Cancel**

- 9 Click **OK** and click **Close** to close the Local Area Connection Properties dialog box

Close the Network Connections window

- 10 Open Internet Explorer and access a Web page

- 11 Close Internet Explorer

- 12 Open the Internet Protocol (TCP/IP) properties again

Reset the IP settings to obtain an IP address and DNS server address automatically

Here's why

To move to the Default gateway box. You're going to continue configuring TCP/IP manually, so you can connect to the Internet.

Default gateway: 192 . 168 . 100 . 1

Preferred DNS server: 204 . 127 . 202 . 4

To open the Advanced TCP/IP Settings dialog box.

You can enter additional IP addressing information here.

DNS server addresses, in order of use:
204.127.202.4

The IP address you entered earlier is displayed. You can enter multiple DNS server addresses, if necessary. You can also configure the DNS suffix here.

You can configure the WINS client here.

You can configure TCP/IP port filtering here.

To close the Advanced TCP/IP Settings dialog box.

To close open dialog boxes and assign the IP addressing information you entered.

To verify that you have network connectivity using the manually assigned IP address.

Windows workgroups and domains

Explanation



Windows computers can be grouped into workgroups and domains. *Workgroups* are just groups of computers that share the same workgroup name. It's more of a means for organizing computers than it is a membership in anything. However, a domain is different. A *domain* is a secure group of computers, printers, and other devices that share a *directory service*: a common database of accounts. Membership in a domain is special: it gives you access to a wide variety of network resources that might not be available to just anybody.

Computers that are joined to a domain as members can be administered through domain administrative accounts and can be configured to allow access through domain user accounts. This makes it easier to share resources, because accounts are kept in a central location. Otherwise, you'd have to maintain accounts on each separate computer. As a CEA-CompTIA DHTI+ technician, you don't have to set up or manage domains, but you do need to know how to join a computer to a domain, log on to a domain, and recognize when a problem with a domain logon might be causing an error that prevents a user from accessing network resources, such as a file server or e-mail.

Joining a workgroup or domain

To join a computer to a workgroup or domain, you need to obtain the workgroup name or the domain's NetBIOS name or DNS name from the network administrator. You also need to be sure that all the DNS properties have been correctly configured.

- In Windows 2000, right-click My Computer and choose Properties. On the Network Identification tab, click Properties, and enter the workgroup or domain name.
- In Windows XP, right-click My Computer and choose Properties. On the Computer Name tab, click Change, and enter the workgroup or domain name.

When joining or exiting a domain, you're required to enter a user name and password with sufficient privileges to perform the action—typically user credentials of a domain administrator. Be sure to have the user name and password handy before you begin this process. You don't need a special user account just to switch workgroups.

*Do it!***A-8: Joining a Windows workgroup**

Here's how	Here's why
1 Click Start , right-click My Computer and choose Properties	To open the System Properties dialog box. You can join a computer to a workgroup at any time, either during Windows installation or after installation is complete.
2 On the Computer Name tab, click Change...	To open the Computer Name Changes dialog box.
3 In the Workgroup box, enter DHTIWKGRP Click OK	To join the classroom workgroup.
4 Click OK twice	
5 Click OK	To close the System Properties dialog box.
6 Click Yes	To restart the computer.

*Do it!***A-9: Viewing network resources**

Here's how	Here's why
1 Click Start and choose My Computer Click My Network Places	
2 Under Network Tasks, click View workgroup computers In the details pane, double-click your partner's computer name	
3 View the network resources on your partner's computer	There is a SharedDocs folder and a link for Printers and Faxes on your partner's computer.
4 Close the open window	

Topic B: Resource sharing

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
1.2	Recognize and implement methods of network security. <ul style="list-style-type: none"> Personal Computer (PC) security
1.3	Configure setup and maintain a residential LAN (Local Area Network). <ul style="list-style-type: none"> Client configuration Resource sharing

Resource sharing

Explanation

You'll be hard-pressed to find a Windows network where users aren't sharing resources of some kind, whether it's spreadsheets and Word documents or the best printer in the office. As a CEA-CompTIA DHTI+ technician, you need to know how to share files and printers, and you need to know how to troubleshoot errors users encounter when trying to share and access shared resources.

Network client software

You can share and access shared folders in all versions of Windows, as long as the necessary components are installed. To share folders and printers, you need *File and Printer Sharing for Microsoft Networks*. To connect to a shared folder or printer, you need the *Client for Microsoft Networks*. You can see both of these components in Exhibit 2-10. If you want to access files or printers on a NetWare server, you need the Microsoft Client for NetWare Networks.

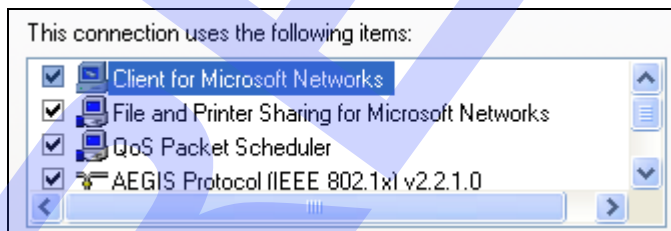


Exhibit 2-10: Components for file sharing

File and folder sharing

File sharing is already accessible in Windows 2000/XP. In Windows XP, you might have to disable Simple File Sharing, which is enabled by default on computers installed into workgroups, to have greater control over NTFS permissions. To disable Simple File Sharing:

- 1 In My Computer, choose Tools, Folder Options.
- 2 On the View tab, uncheck “Use simple file sharing.”
- 3 Click OK.

To share a file or folder on a Windows computer:

- 1 In Windows Explorer, right-click the file or folder and choose Properties.
- 2 On the Sharing tab, enable sharing.
- 3 Enter a share name, if you don’t want to use the default share name. (Sharing folders is easier to manage than sharing files.)
- 4 Click OK.

Do it!

If Simple File Sharing hasn’t been disabled, have students disable it now. The Windows Firewall should be configured to allow file and printer sharing.

B-1: Sharing a folder**Here’s how**

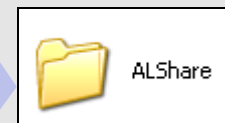
- 1 Open My Computer
- 2 On drive C:, create a folder named **NNShare**
- 3 Right-click the new folder and choose **Sharing and Security...**
- 4 Click **If you understand the security risks but want to share files without running the wizard, click here**

Select **Just enable file sharing**

Click **OK**

Here’s why

You’re going to create and share a folder—pretty common practice in offices that need to share information among many people.



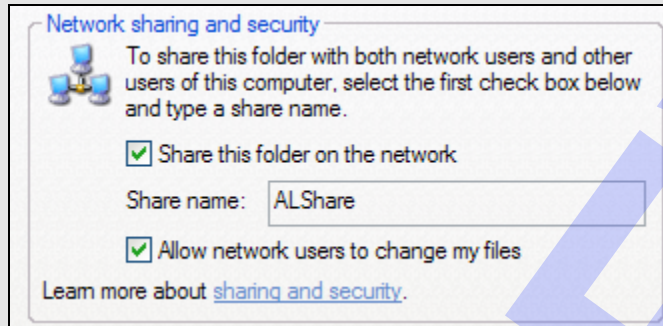
Enter your initials instead of “NN.”

To open the folder’s Properties dialog box with the Sharing tab activated.

If the Share this folder on the network option is not shown.

- 5 Select **Share this folder on the network**

Select **Allow network users to change my files**



Leave the default share name

- 6 Click **OK**

- 7 Observe the folder's icon



The hand indicates that the folder is shared.

Connecting to shares

Explanation



You can connect to a share by using Network Neighborhood or My Network Places to browse to the computer that holds the share, or you can click Start, choose Run, and enter the Universal Naming Convention (UNC) path to the share. The format for the UNC is \\computername\sharename.

Do it!

B-2: Connecting to a shared folder

Assign students to work in pairs. If you have an odd number of students, have one student work with you. Make sure students know their computer names.

Here's how	Here's why
1 Talk to your partner and find out his or her computer name	You're going to use a UNC path to connect to another student's shared folder. This is the most direct way to connect to a Windows share over the network.
2 Click Start and choose Run...	
3 Enter \\computername	Where <i>computername</i> is the name of your computer. Share names and computer names are not case-sensitive.
4 Click OK	To access your partner's computer.
5 Observe the shared folder	It's listed with the Printers and Faxes folder and the Scheduled Tasks folder. Note the name of the share.
6 Close the window	
7 Click Start and choose Run... Enter \\computername\share	(Where <i>computername</i> is the name of your computer, and <i>share</i> is the name of the share.) To connect to the share directly.
8 Close the window	

Shared printers

Explanation



You share printers in much the same way you share folders. To share a printer, right-click it and choose Properties. On the Sharing tab, choose to share the printer, and add a share name, if you don't want to use the default share name. Users can print to a shared printer but can't manage (pause, delete) print jobs by default. For that, you need to assign users additional permissions.

To connect to a shared printer, browse to the computer with the shared printer through Network Neighborhood or My Network Places. You can then drag the shared printer to your desktop or right-click the printer and choose Connect.

Do it!

B-3: Sharing a printer

Students should have printer drivers installed. (The printer drivers make it appear as if a printer is installed, even if one isn't attached to the computer.) If students don't have a printer installed, have them install one now.

Here's how	Here's why
1 Click Start and choose Printers and Faxes	You're going to share a printer. If Printers and Faxes is not listed on the Start menu, open Control Panel, click Printers and Other Hardware, then click Printers and Faxes.
2 Right-click an installed printer and choose Sharing...	
3 Select Share this printer and leave the default share name	The printer share name is limited to eight characters by default for backward compatibility with older applications.
4 Click OK	The printer icon has a hand on it.
5 Close all open windows	

*Do it!***B-4: Connecting to a shared printer****Here's how**

1	Work with your partner to connect to exchange printer information	
2	Open Printers and Faxes	
3	Click Add a printer	In the Printer Tasks list.
4	Click Next	To start the Add Printer Wizard.
	Select A network printer, or a printer attached to another computer	
	Click Next	
5	With Browse for a printer selected, click Next	
6	Double-click your partner's computer name	You might need to double-click the workgroup name first.
	Select your partner's printer	
	Click Next	
7	Click Yes	To automatically install the print driver on your machine.
8	Select No	To not set the printer as the default printer.
	Click Next	
9	Click Finish	The printer is now listed in your Printers and Faxes window.
10	Close all open windows when you're done	MoreInfo

Topic C: Internet connectivity

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
1.1	Identify basic networking protocols and their uses and know when/how to apply them. <ul style="list-style-type: none"> • DNS • TCP/IP
1.2	Recognize and implement methods of network security. <ul style="list-style-type: none"> • Personal Computer (PC) security
1.3	Configure setup and maintain a residential LAN (Local Area Network). <ul style="list-style-type: none"> • Network device setup and integration • Broadband configuration (such as DSL, cable, and satellite)
1.4	Configure setup and maintain a secure wireless network. <ul style="list-style-type: none"> • Differentiate applications of hardwired vs. wireless networks
1.5	Identify and define network cabling characteristics and performance <ul style="list-style-type: none"> • Cable types <ul style="list-style-type: none"> • CAT5 • CAT5e • CAT6 • Fiber • COAX • Protocols <ul style="list-style-type: none"> • 10BaseT • 100BaseT • 1000BaseT • Shielded (STP) vs. unshielded (UTP) • Plenum vs. non-plenum • Importance of conductor colors

Internet technologies

Explanation

In today's world, the Internet is business, and business is the Internet. There's hardly an organization around that doesn't have an Internet presence and most (if not all) organizations nowadays connect to the Internet in some way, even if it's just to send and receive e-mail. Most organizations use the Internet for much more, and as a CEA-CompTIA DHTI+ technician, you're responsible for configuring and troubleshooting user Internet access.



Basic terminology

Although there's some overlap between networking concepts and Internet concepts and terminology (after all, the Internet is just a huge TCP/IP network), there are some terms worth highlighting for prospective CEA-CompTIA DHTI+ technicians. The following table explains these terms.

Term	Description
Internet service provider (ISP)	A company that sells Internet access to an organization. An ISP provides the connection to the Internet and might also provide other services, such as server space for a company to host a Web site or store data files.
E-mail	<p>A form of electronic communication where text messages are sent and received from computers, personal digital assistants (PDAs), or cell phones. E-mail clients, such as Outlook or Eudora, are used to create, send, and receive e-mail. E-mail messages are processed through e-mail servers, such as Microsoft Exchange or Lotus Domino, within each organization or ISP.</p> <p>There are three e-mail protocols:</p> <ul style="list-style-type: none"> • Post Office Protocol (POP) — Used to retrieve e-mail from an e-mail server. Used with SMTP, although POP version 3 (POP3) can be used without SMTP. • Internet Message Access Protocol (IMAP) — Used to retrieve e-mail from an e-mail server. Used with SMTP, although IMAP4 can be used without SMTP. • Simple Mail Transfer Protocol (SMTP) — Used to send e-mail to an e-mail server. Used with POP or IMAP.
Hypertext Markup Language (HTML)	Used to format Web pages for transfer and display in Web browsers such as Internet Explorer or Firefox.
DNS	Domain Name Service is the service that maps names to IP addresses. DNS makes it easy to use familiar names rather than unfamiliar IP addresses.
World Wide Web	The collection of computers and servers used to store and share information on the Internet in the form of Web pages. The Web isn't synonymous with the Internet. The Internet is the vast, global network of computers, of which the Web is just one part, one way of communicating. Other services and means of communicating on the Internet include e-mail, newsgroups, and instant messaging.

A good way to remember that SMTP is used to send messages is the mnemonic "Send Mail To People."

Internet protocols

The following table describes some of the protocols that are used on the Internet.

Protocol	Description
TCP/IP	The protocol of the Internet.
Hypertext Transfer Protocol (HTTP)	The protocol used to make Web requests and download Web pages over TCP/IP.
Secure Sockets Layer (SSL)	A public-key/private-key encryption protocol used to transmit data securely across the Internet over TCP/IP. Web sites that require SSL begin with https://, rather than the usual http://. When you connect using SSL, the connection itself is secure, and so is any data transferred across the connection.
Secure HTTP (S-HTTP)	Another protocol used to secure Internet transmissions. Whereas SSL secures a connection between two computers, S-HTTP secures the individual data packets themselves.
Telnet	A terminal emulation protocol used over TCP/IP networks. You can use Telnet to connect to a remote server across the Internet. You can then enter commands on your computer, and the commands are executed as if you were entering them into the server directly. Telnet is used mainly for remote management of servers and other devices, such as routers.
File Transfer Protocol (FTP)	FTP is used to transfer files to and from an FTP server over a TCP/IP network.

ISP connection technologies

A LAN has much less need for data throughput than does a national backbone. Lying between these two extremes on the spectrum are many types of systems that require varying degrees of bandwidth. Exhibit 2-11 illustrates various types of networks and their bandwidths.

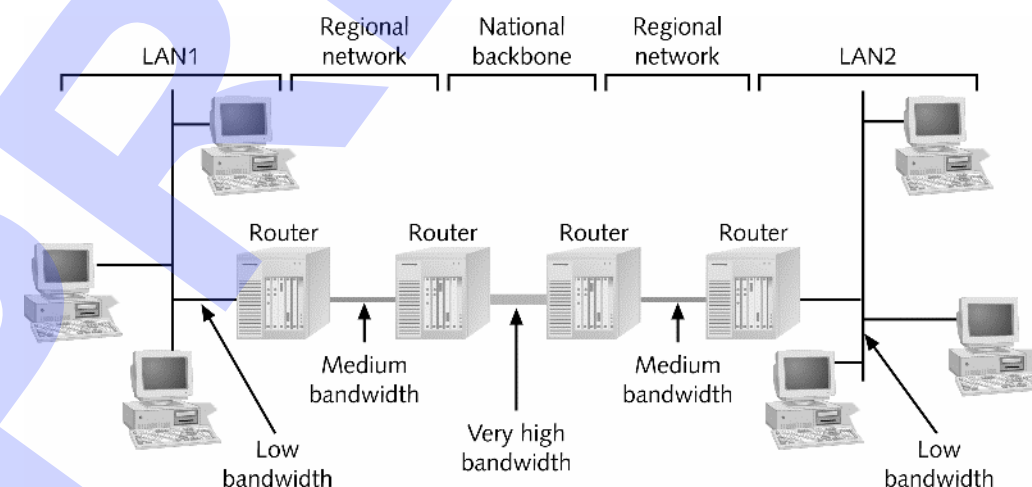


Exhibit 2-11: The Internet infrastructure

Regular telephone lines

Regular telephone lines, one of the most common ways to connect to an ISP, require an internal or external modem. A modem converts the computer's digital data (data made up of zeros and ones) to analog data (a continuous and infinite number of variations of frequencies) that can be communicated over telephone lines. As data travels from the computer to the modem, it's converted from digital to analog. On the receiving end, as it travels from the modem to the computer, it's converted from analog back to digital.



Use this slide to explain the concepts pertaining to Internet connections over regular phone lines.

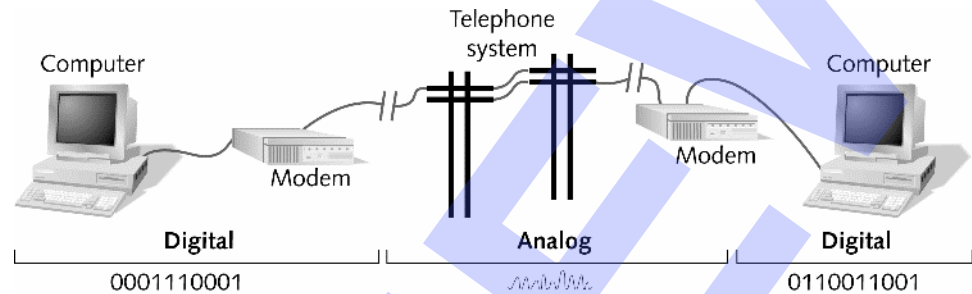


Exhibit 2-12: Communication via PSTN

When data packets are traveling over telephone lines, the Data Link layer protocol used is *PPP (Point-to-Point Protocol)* or *SLIP (Serial Line Internet Protocol)*. PPP most often is used to transmit TCP/IP packets from a computer connected to an ISP or intranet access point by telephone line. PPP encloses a TCP/IP packet within its own header and trailer information. This header and trailer information is used only while the packet travels on the telephone line. After it's off the line, the PPP header and trailer information is stripped from the packet before it continues over the network. The TCP/IP frame is enclosed in the PPP header and trailer and then presented to the modem for delivery over telephone lines to a modem on the receiving end. The modem on the receiving end passes the packet to the PPP utility, which removes the PPP header and trailer information before sending the packet on its way.

An earlier version of a line protocol is SLIP, which also supports a TCP/IP network but seldom is used today. SLIP doesn't support authentication or other security features, including encrypted passwords.

The telephone system is carrying analog data from modem to modem, which seldom occurs on actual systems. The data is analog only from a customer's telephone or modem to the telephone company's central office, where it's converted to digital until it reaches the central office of the recipient. If the recipient is an ISP that's using regular telephone lines to connect to its customers, the data is converted to analog for the final leg of its journey from the ISP's central office to the ISP modem. Because of the standards used by the telephone companies to convert from digital to analog or analog to digital, the fastest possible transmission over telephone lines is 56 Kbps (56,000 bits per second), although speeds this fast are rarely attained, even when both the user and the ISP are using 56K modems. New technology has opened the way for faster and more advanced methods of communication.

Cable modem

Cable modem communication uses cable lines that already exist in millions of households in the United States. Just as with cable TV, cable modems are always connected. A cable modem is an example of *broadband media*. Broadband refers to any type of networking media that carries more than one type of transmission. With a cable modem, the TV signal to your television and the data signals to your computer share the same cable.

Cable television lines are analog. A cable modem converts your computer's digital signals to analog before sending data out on the cable television line and also converts incoming data (from the television cable or the telephone line) from analog to digital. Cable modems primarily use a technology called DOCSIS (data over cable service interface specifications).

Unlike a telephone line, which creates a single, point-to-point connection between your house and the telephone company facilities, a cable coming to your home doesn't provide a single point-to-point connection. Instead, a cable establishes a *point-to-multipoint* connection, whereby the signal from the cable company is sent to multiple destinations. Your connection is one of many in the neighborhood that all tie to a single backbone cable coming into the neighborhood. For this reason, you can see degradation in service if many people are using cable modems in your area and are competing for the same bandwidth.

Another disadvantage of cable modems is the lack of security between you and the cable company ISP, because many users are sharing this connection with you. For this reason, if you use a cable modem, you might want to use a personal firewall to protect your computer from hackers.

When you lease cable modem service, you are most likely also agreeing to use the cable modem company as your ISP. The cost for cable modem service including ISP cost is in the range of \$20 to \$60 per month.

PPPoE (Point-to-Point Protocol over Ethernet)

When you set up either a cable or DSL connection for your computer, you need to use a converter box that sits between your computer and the DSL line or TV cable line. For cable modems, the converter box is called the cable modem, and for DSL, the box is called the DSL converter box. (Sometimes, a router is used in place of a DSL converter box.) This device connects to your computer using an Ethernet cable that plugs into an Ethernet NIC in your computer, as shown in Exhibit 2-13. The PPPoE protocol carries the data packets over this short Ethernet link from your computer to a broadband connection.

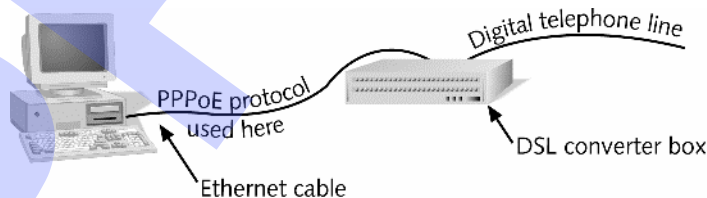


Exhibit 2-13: PPPoE

Remind students that PPP is the protocol that allows TCP/IP packets to travel over telephone lines.

PPPoE (Point-to-Point Protocol over Ethernet) is a protocol that adapts PPP to work with Ethernet. PPPoE describes how the computer is to interact with the converter box or modem when the two are connected by an Ethernet cable connected to an Ethernet network card in the computer. PPPoE gives the user the security and authentication that's offered with PPP. PPPoE also sets standards for networks to connect to the Internet via DSL modems and other high-speed access services.

ISDN

ISDN (Integrated Services Digital Network) is a technology developed in the 1980s that uses regular telephone lines and is accessed by a dial-up connection. ISDN is actually an early implementation of DSL. For home use, an ISDN line is fully digital and consists of two channels, or telephone circuits, on a single pair of wires called B channels and a slower channel used for control signals, called a D channel. Each B channel can support speeds of up to 64,000 bps. The two lines can be combined so that, effectively, data travels at 128,000 bps, which is about three to five times the speed of regular telephone lines.

ISDN requires an ISDN converter box that provides an Ethernet connection to the computer, or you can use an ISDN card installed inside the computer. ISDN is expensive for home and small business Internet connections and is being replaced by DSL, which is a faster and less expensive solution for Internet access.

DSL

The telephone industry has developed several similar technologies that collectively are called DSL (Digital Subscriber Line). DSL is fast data transmission technology, which is affordable for home use and offers a direct connection rather than a dial-up. It's a broadband technology that uses ordinary copper telephone lines and a range of frequencies on the copper wire that aren't used by voice, making it possible for you to use the same telephone line for voice and DSL at the same time. The voice portion of the telephone line requires a dial-up as normal, but the DSL part of the line is always connected.

Because DSL uses regular telephone lines, it's point-to-point. That means you don't need to be concerned that you're competing with others in your area for bandwidth, as is the case with cable modems. The cost of a DSL line varies greatly, from \$35 to \$85 per month, depending on your location.

Satellite

People who live in remote areas and want high-speed Internet connections are often limited in their choices. DSL and cable modems might not work where they live, but satellite access is available from almost anywhere. Technology is even being developed to use satellites to offer Internet access on commercial airlines. Customers can use their own laptops to connect to the Internet through a connection at their seats to a satellite dish in the airplane.

A satellite dish mounts on top of your house or office building and communicates with a satellite that's used for communication by an ISP offering the satellite service. Originally, satellite access was only one-way. Data was sent to the users via satellite, but data transmitted from the users to the servers was sent over the telephone lines. This was usually acceptable because, for normal Internet use, the amount of data transmitted from the client is small when compared with what's sent from servers to the client.

A computer using this system connects to a satellite modem, which connects to a satellite dish on the house. The computer also is connected to the ISP by telephone line.

When a request is made to a Web site, the request is sent through the telephone line. The ISP receives the request and then sends the response through the satellite.

New technology allows data to be transmitted both ways over the satellite so that telephone line connections aren't needed. An external satellite modem providing two-way transmission has two interface cards each with a cable connection, one for sending and one for receiving data. The modem box connects to the computer by using either an Ethernet connection to a NIC installed in the computer or a USB port, which is a standard port on most computers. Data in both directions is transmitted via satellite. For remote users, this often eliminates a long-distance telephone call.

Several companies offer satellite Internet access. The average setup cost is around \$600 with monthly fees starting at \$60.

Wireless

The term "wireless" refers to several technologies and systems that don't use cables for communication, including public radio, cellular telephones, one-way paging, satellite, infrared, Bluetooth, and private, proprietary radio. Because of the expense and the concern that increasing the use of wireless might affect our health, airplane control systems, pacemakers, and other similar things, wireless isn't as popular as wired data transmission. Wireless is an important technology for mobile devices and for Internet access in remote locations where other methods aren't an option.

For Internet access, two popular applications of wireless are:

- Fixed-point wireless, sometimes called Wireless Local Loop (WLL)
- Mobile wireless

With fixed-point wireless, an antenna sits on your house or office building and communicates with a base station antenna. With mobile wireless, a wireless modem connects to a laptop computer and communicates with a grid of transmitters spread over a wide geographical area, forming a wide area network (WAN). This grid is called a wireless WAN.



Use this slide to explain Wireless WAN concepts.

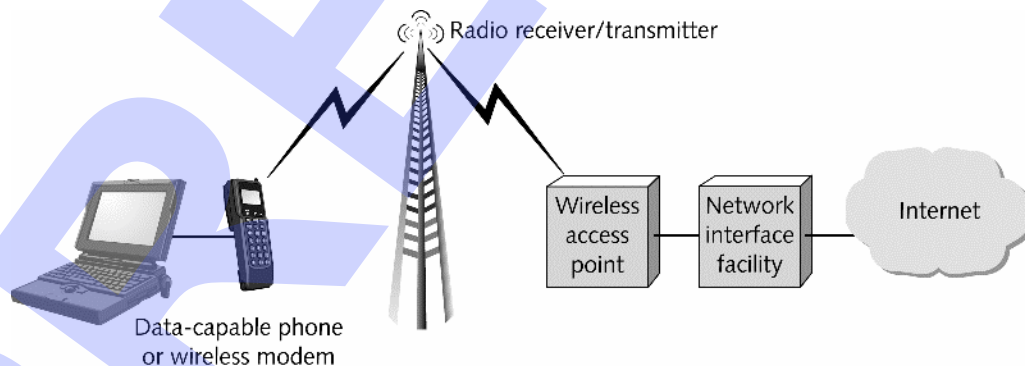


Exhibit 2-14: Wireless WAN

Remote access methods

Home users have remote access to many systems these days. They might have been given access to servers at work. Many libraries offer remote access to the card catalog and online databases. Students might need to access servers at school. The remote server usually requires that the user have a valid username and password. It might also require that the user account is set up to allow remote access.

Any of the methods of connecting a home LAN to the Internet can be used to make a remote access connection.

Do it!

C-1: Identifying Internet technologies

Questions and answers

- 1 Which of the following is the protocol of the Internet?
 - A HTTP
 - B TCP/IP**
 - C HTTPS
 - D SSL
- 2 Which of the following protocols retrieve e-mail messages from an e-mail server? (Choose all that apply.)
 - A IMAP4**
 - B SMTP
 - C POP3**
 - D HTTP
- 3 Which of the following protocols send e-mail messages to e-mail servers? (Choose all that apply.)
 - A IMAP4**
 - B IMAP
 - C POP3**
 - D SMTP**
- 4 Which protocol secures connections between two computers?
 - A SSL**
 - B TCP/IP
 - C FTP
 - D Telnet
- 5 Which connectivity technology uses digital telephone lines exclusively?
 - A DSL
 - B ISDN**
 - C WLL
 - D Cable
- 6 What are two ways of making a wireless connection to the Internet?

First, a user can connect to a wireless hotspot in a building, provided by a business, such as a coffee shop or airport, or a hotspot provided by a municipality. Second, a user can connect to the Internet by using a cellular telephone network.

7 Why might you use Telnet to connect to a remote server? Give an example.

To administer that server from another location, for example, from home or from a branch office.

8 What's the difference between HTML and HTTP?

HTML is a coding language used to format Web pages. HTTP is the protocol used to connect to a Web site and download a Web page.

9 How does TCP/IP relate to other protocols, such as SSL and HTTP?

These other protocols run on top of the TCP/IP network.

Do it!

Discuss with students why they feel their answer is the best choice in each scenario.

C-2: Selecting a connection technology

Exercises

1 For each user, select the appropriate connection technology.

Susan is a salesperson who travels extensively. She needs to be able to send and receive communication to the home office and clients while in transit. What's Susan's best choice for connection technology?

Wireless. Many locations, such as coffee houses, airport terminals, and other public buildings, have wireless access points that Susan could use to connect to her company's LAN through the Internet.

James is an architect who works out of his home in the Adirondack mountains. James must send and receive large CAD drawings to/from clients and builders. What's James' best choice for connection technology?

Because of James' remote location, he's probably too far away to connect via cable or DSL lines. Dial-up service using PSTN would likely be terribly slow uploading and downloading the CAD drawings. Although it might be more expensive, James' best bet would be satellite service with transfer speeds that are the same for uploading and downloading.

Grace lives next to James in the Adirondacks. She's retired and uses e-mail to communicate with her children and grandchildren all over the country. Sometimes they send her digital pictures attached to the e-mail messages so she can see the grandchildren. She occasionally uses her Web browser to look up information. What's Grace's best choice for connection technology?

Grace's livelihood doesn't rely on her Internet connection. She doesn't send large files and receives picture files occasionally. An inexpensive dial-up service using the phone lines already connected to Grace's house would serve her needs just fine.

Internet connections

Explanation

CEA-CompTIA DHTI+ technicians are generally asked to configure and troubleshoot two types of user Internet connections: those made from the workplace and those made from a remote location, typically a user's home. It's important to note that CEA-CompTIA DHTI+ technicians typically aren't responsible for connecting an entire LAN to the Internet or troubleshooting that connection. That task is left to network administrators and engineers. Your job is to ensure that users can connect to the Internet from their Windows computers. Any network configuration beyond the desktop is left to other individuals.

LAN Internet connections

In a workplace or office, a user connects through the organization's LAN. A connection through the LAN requires a valid network connection, and that requires, at a minimum, a working network card, an IP address, and a subnet mask. In addition, you need to add the IP address of a *gateway*, which is generally the server or router that connects the LAN to the Internet. In larger networks, the gateway might just be a router on the same network segment that eventually forwards the packets to the Internet gateway. You might also need to add the IP addresses of one or more DNS servers.

In all Windows operating systems, to configure TCP/IP settings, open the TCP/IP properties of the network connection, or configure the computer to use DHCP and make sure the necessary information is configured on the DHCP server. Exhibit 2-15 shows TCP/IP properties configured for Internet access through a LAN.

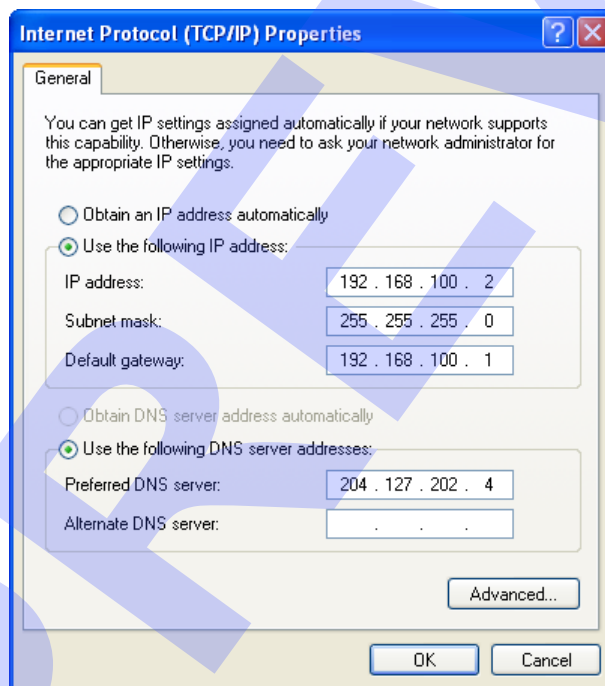


Exhibit 2-15: TCP/IP connection properties for access through a LAN

If you're connecting users to a wireless LAN, you need the necessary wireless information, such as the name of the wireless network and any passwords or encryption keys used to secure wireless access.

*Explanation***Physical network components**

Data flow on a network is influenced and controlled by the physical components (or parts that make up the network). Depending on the traffic patterns that are desired, different components need to be used.

Media

One of the most visible parts of a network is the media, which is the physical component that connects all of the devices together. Each type of media has varying benefits and limitations. The most common media types used in computer networks are:

- Twisted-pair
- Fiber optic
- Coaxial
- Wireless

Twisted-pair

Twisted-pair cabling is the most common type of cabling used in computer networks. When used on an Ethernet network, it can carry data at up to 1 Gbps at a maximum distance of 100 meters over a single segment. This type of cabling is inexpensive, and many qualified installers are available.

While there are different specifications for twisted pair, all of them include two or more pairs of wire, twisted together and housed in a single protective sheath. The installation environment and media access method will determine which type of twisted-pair cable is appropriate for each application.

Twisted pair is made of insulated copper wires that have been twisted around each other to form wire pairs. Usually the wire is #22 to #26 gauge, and more than one pair can be carried in a single jacket or sheath. When working with twisted pair, note the difference between a wire and pair. A two-pair cable has four wires.

Because wire carrying electricity transmits and receives electromagnetic energy, nearby pairs of wires carrying signals can interfere with each other. This is called *crosstalk*. To reduce crosstalk and other electromagnetic interference (EMI) sources, the wires are twisted.

The number of twists and interim spacing are specified by industry standards organizations. Standard commercial-grade communications cable supports two twists per 11 inches.

Cables with a greater number of twists within the 11-inch measure can support data transmissions at higher speeds and greater distances. The exact distance specifications depend on the terminating equipment that is used.

Twisted-pair cabling is divided into two categories:

- Unshielded twisted pair (UTP)
- Shielded twisted pair (STP)

UTP, as shown in Exhibit 2-16, is a set of twisted pairs within a plastic sheath. The common use for this type of cable is telephone wiring and LAN communications.

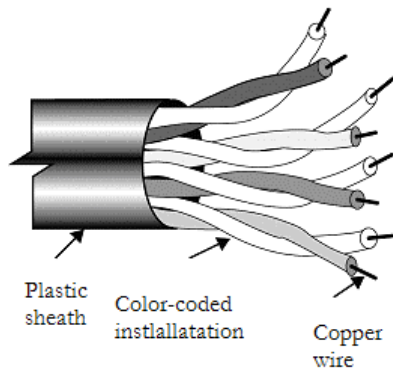


Exhibit 2-16: Unshielded twisted pair (UTP)

A number of wiring classification schemes are in use. Common schemes are the levels from Underwriter's Laboratory (UL) and categories from the Electrical Industries Association.

The two older popular UTP cabling types are Category 3 and Category 5 UTP. Both cable types are designed to support #24 AWG (American Wire Gauge). Category 3 cable supports data transport rates from 10 Mbps to 100 Mbps depending on the installation. However, at 100 Mbps, imperfections in Category 3 cable can cause network problems due to EMI. Category 5 cable is designed with more twists per foot and better insulation than Category 3, enabling it to more reliably support data transport rates up to 100 Mbps. Newer to the scene are Category 5e and Category 6 UTP. Both have been designed to more stringent specifications and can support transmission speeds of up to 1,000 Mbps, so they can support Gigabit Ethernet. Any new installation of UTP cabling should be done with a minimum of Category 5e cable.

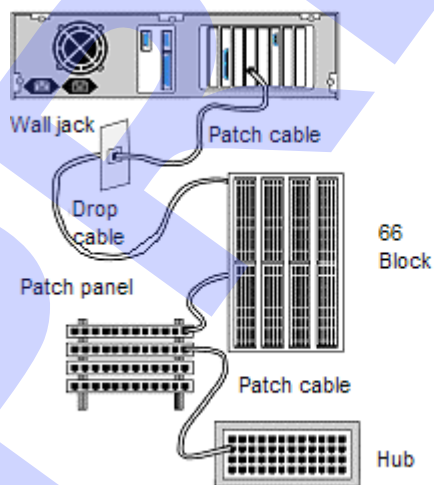


Exhibit 2-17: A typical UTP installation

Some facts to remember about UTP include:

- Cost. Low cost compared to other media, typically running about 25–30 cents per foot.
- Ease of installation. Relatively easy to install, requiring only a few specialized tools (crimpers and a punch-down tool).
- Capacity. Data transfer rates from 1 to 1,000 Mbps with 10 and 100 Mbps being the most common.
- Attenuation. Rapid attenuation, distance limited to hundreds of meters.
- EMI immunity. Susceptible to EMI.

STP includes a protective sheathing around the copper wire. The twisted pair is wrapped in foil to cut down on outside interference and electromagnetic radiation. STP has many of the same characteristics of UTP. However, it is designed for #22 AWG wire, which has a thicker wire core and supports longer distances than the #24 AWG variety.

Some facts to remember about STP include:

- Cost. Moderate cost (approximately 20–40 cents per foot).
- Ease of installation. The shield in STP cable must be grounded, making installation more difficult than UTP. Special connectors and installation techniques are needed. The use of pre-configured cable and connectors makes this easier.
- Capacity. With the reduction of external interference, greater transmission speeds (up to 500 Mbps) can be implemented. Some 155-Mbps cabling exists, but the common transmission rate is 16 Mbps.
- Attenuation. Similar to UTP. Distance is limited to 100 m for 500 Mbps, longer for lower speeds.
- EMI immunity. The foil shielding reduces both interference and EMI emissions. STP will still suffer from outside interference, but not as much as UTP.

Twisted pair cabling usually is terminated using an RJ-45 connector. It connects eight wires within the cable to the jack. The EIA/TIA-568-A standard defines two wiring patterns for Ethernet CatX cabling. These are T568A and T568B. These standards specify the pattern in which the color-coded wires in the cable are connected to the pins of the RJ-45 connector or the jack.

If you hold an RJ-45 connector in your hand with the tab side down and the cable opening toward you, the pins are numbered from left to right: 1 through 8. The pin numbers connect to the following colored wires in the cable for T568A and T568B.

The following table shows how the colors are usually designated in wiring diagrams and instructions.

Pin	T568A standard	T568B standard
1	Green/White	Orange/White
2	Green	Orange
3	Orange/White	Green/White
4	Blue	Blue
5	Blue/White	Blue/White
6	Orange	Green
7	Brown/White	Brown/White
8	Brown	Brown

T568A standard is preferred for residential applications and T568B for commercial applications. Both, however, are electrically identical as long as you use the same color pattern to connect both ends of a given cable. If you are consistent, pin 1 at one end of a cable is always connected to pin 1 at the other end, and pin 2 on one end is connected to pin 2 on the other end, and so on, regardless of which of the two color patterns you use.

For the network you're working on, pick one standard and use it for all the wiring. It doesn't matter which you choose. If you were to buy a pre-made Cat5 patch cable that has been made to the other standard, it will still work on the network because both ends of the cable are wired to the same standard.

Fiber optic

Fiber optic cabling is commonly used for network backbones where twisted-pair cabling cannot transmit the distance that is required. When used with an Ethernet network, it can carry data at up to 10 Gbps at a maximum distance of 2 kilometers. This type of cabling is more expensive than twisted-pair and fewer qualified installers are available. Two fibers are required for each connection. One fiber is used for sending data, and the other for receiving.

Coaxial

Coaxial cabling was common on older Ethernet networks but has been removed from most networks. Newer fast standards were never developed for coaxial cable and the maximum speed available is 10 Mbps. Other disadvantages of this type of cabling include the inability to transmit in full-duplex mode, and in common implementations, all computers are on a bus topology with only one collision domain. Coaxial cabling is now relatively expensive compared to twisted-pair cabling.

Coaxial cable is used to connect to a cable television connection. It is also used to access cable modems that deliver high speed Internet access.

Wireless

Wireless connectivity is not part of the Ethernet standard. However, many switches are available that have Ethernet connections and wireless capability to facilitate communication between Ethernet and wireless networks. The network cards for wireless networks are more expensive than twisted-pair, but less than the price of fiber optic network cards. A major cost savings in wireless implementations is the lack of cabling installation, although security is a major concern.

Wiring the network

Wiring is the backbone of a network. It is also the part most vulnerable to performance problems caused by poor installation practices. Wiring in new construction is generally a straightforward process, but it needs to be carefully and precisely done if the wiring is to perform at capacity and endure for years. Wiring in existing structures, whether done within the walls or on the surface, can be a frustrating experience, but this type of wiring needs to be as professionally installed as that in new construction. Forcing cables around corners and through openings too small to accept them many enable an installer to get a connection made, but a forced connection rarely performs up to standard. No network is better than the quality of the wiring on which it runs.

Wiring is often done through the walls in new construction. In modifying existing structures to have a wired network, it may be a combination of through-the-wall and surface-mounted wiring. Surface mounted wiring is usually run through a raceway or under molding. Cutting a groove in the back of chair rail, ceiling or baseboard moldings provides a way to conceal the wiring while having enough space for the wire behind the molding.

Plenum wiring

A plenum is an enclosure in a building that is used to move air for heating, cooling, or humidity control. It may be created by a false ceiling, a false floor, metal duct work or a variety of other construction methods, but its main purpose is to move air that is environmentally controlled in some manner. A secondary purpose of a plenum may be to contain high or low voltage wiring. Because plenums often connect rooms in a building, they provide convenient paths through which to run wiring.

Cables run in plenums must meet applicable fire protection and environmental requirements. These are important because the plenum-run cables may be subjected to temperature and humidity extremes not encountered in normal wiring paths. Plenum wiring also poses a greater hazard than wiring run inside walls because, if a fire occurs in the plenum-run wiring, smoke and heat will be carried by the moving air in the plenum to other parts of the building, thus spreading the fire faster than it would otherwise move.

Protection for plenum-run cables may mean enclosing them in conduit (inside the plenum) or using cables having jackets and other components made of materials that are resistant to open flame and are non-toxic at high temperatures. Plenum cabling is often covered with Teflon and is more expensive than ordinary cabling. In the event of fire, its outer material is more resistant to flames, and when burning, produces less smoke than ordinary cabling. Twisted pair and coaxial cable are both made in plenum cable versions.

Ethernet topologies

Ethernet networks can be wired with different types of cable, each with its own benefits and drawbacks. Some of the specifications for Ethernet topologies are the following:

- 10Base-T — Baseband specification that uses Category 3 or better UTP cable. This cabling medium can carry a message for 100 m (about 328 feet) between a computer and a hub. It operates at a speed of 10 Mbps and uses an RJ-45 connector.
- 10Base-FL — Baseband specification that uses fiber optic cable. This cabling medium can carry a message for up to 2,000 m between a computer and a repeater hub. It operates at a speed of 10 Mbps and can use different connectors, such as ST or SC connectors.
- 100Base-TX — Baseband specification that uses Category 5 UTP or STP cable. This cabling medium can carry a message for 100 m (about 328 feet) between a workstation and a hub. It operates at a speed of 100 Mbps and uses an RJ-45 connector.
- 100Base-FX — Also known as FDDI. Baseband specification that uses fiber optic cable. This cabling medium can carry a message for 2,000 m between a workstation and a repeater hub. It operates at a speed of 100 Mbps.
- 1000Base-TX — Gigabit Ethernet specification that runs over Category 5 UTP cable at 1,000 Mbps with a maximum segment length of 100 meters.
- 1000Base-CX — Gigabit Ethernet specification that runs over STP cabling at 1,000 Mbps with a maximum segment length of 25 m.
- 1000Base-SX — Gigabit Ethernet specification that runs over fiber optic cable at 1,000 Mbps with a maximum segment length of 550 m.
- 1000Base-LX — Gigabit Ethernet specification that runs over Category 5 UTP cable at 1,000 Mbps with a maximum segment length of up to 5,000 m.
- 10Base-SR — 10 Gigabit Ethernet specification that runs over multimode fiber optic cable at 10,000 Mbps with a maximum segment length of 82 m. Operates in full duplex mode.
- 10Base-LR — 10 Gigabit Ethernet specification that runs over single mode fiber optic cable at 10,000 Mbps with a maximum segment length of 10 kilometers.
- 10Base-ER — 10 Gigabit Ethernet specification that runs over single mode fiber optic cable at 10,000 Mbps with a maximum segment length of 40 kilometers. Operates in full duplex mode.

Note that a typical use for Gigabit Ethernet would be on a business or academic campus, where the fiber backbone would connect the buildings at 1,000 or 10,000 Mbps, while within the buildings copper connects individual PCs at 10 or 100 Mbps.

Do it!

C-3: Discussing network media

Questions and answers

1 Which type of media has the most security concerns?

Wireless

2 Which type of media can carry Ethernet signals up to 2 kilometers?

Fiber optic

3 Shielded twisted-pair cable can run at speeds up to:

- A 10 Mbps
- B 100 Mbps
- C 200 Mbps
- D 500 Mbps**

4 _____ is made of insulated copper wires that have been twisted around each other to form wire pairs.

Twisted pair

5 Explain crosstalk.

Wires carrying electricity transmit and receive electromagnetic energy. This can cause nearby pairs of wires carrying signals to interfere with each other. Such interference is called crosstalk.

Topic D: Network protection

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
1.1	Identify basic networking protocols and their users and know when/how to apply them. <ul style="list-style-type: none"> • UDP
1.2	Recognize and implement methods of network security. <ul style="list-style-type: none"> • Personal computer (PC) security • Antivirus • Home networking security • Firewall knowledge
1.4	Configure setup and maintain a secure wireless network. <ul style="list-style-type: none"> • Differentiate applications of hardwired vs. wireless networks • Access networking security and encryption standards <ul style="list-style-type: none"> • WEP • WPA • MAC filtering • SSID • WPA2 • Wireless networking integration and troubleshooting <ul style="list-style-type: none"> • Frequency management • Wireless protocol standards <ul style="list-style-type: none"> • 802.11 a/b/g/n

Firewalls

Explanation



One of the most important things to do when setting up a computer, a server, or a LAN is to install a firewall. A *firewall* is software or hardware used to control information that's sent and received from outside the network. The firewall resides on the network's gateway, which is the connection point between the internal network and outside communication. The firewall ensures that all communication is received from outside users and computers that are legitimate. A firewall can be installed on several different types of gateways, including a router, server, or computer. Firewalls can be used to help prevent DoS attacks and infections from viruses, worms, or Trojan horses.



Various types of firewalls can function in several ways:

- Firewalls can filter data packets, examining the destination IP address or source IP address or the type of protocol used by the packet (for example, TCP or UDP).
- Firewalls can filter ports so that outside clients can't communicate with inside services listening at these ports.
- Firewalls can filter applications, such as FTP, so that users inside the firewall can't use this service over the Internet.
- Some firewalls can filter information, such as inappropriate Web content, for children or employees.

In addition, some firewalls can set alarms, when suspicious activities happen, and track this activity in log files. Several variations of firewalls are available, from personal firewalls to protect a single computer up to expensive firewall solutions for large corporations. When selecting a firewall, know what's being filtered, how it's filtered, and what options the firewall offers.

Hardware firewall

A good firewall solution is a hardware firewall that stands between a LAN and the Internet. (See Exhibit 2-18.) A hardware firewall is ideal for a home network consisting of two or more computers because it protects the entire network. For most home and small-office LANs that connect to the Internet through a single cable modem or DSL converter, a broadband router is used as a hardware firewall. You can buy a broadband router with enough ports to connect several computers and perhaps a network printer to it. Some broadband routers also serve double duty as a wireless access point to the network, DHCP server, and proxy server. The broadband router connects directly to the cable modem or DSL converter. Note that some DSL devices are also broadband routers and include embedded firewall firmware.



Use this slide to explain hardware firewall concepts.

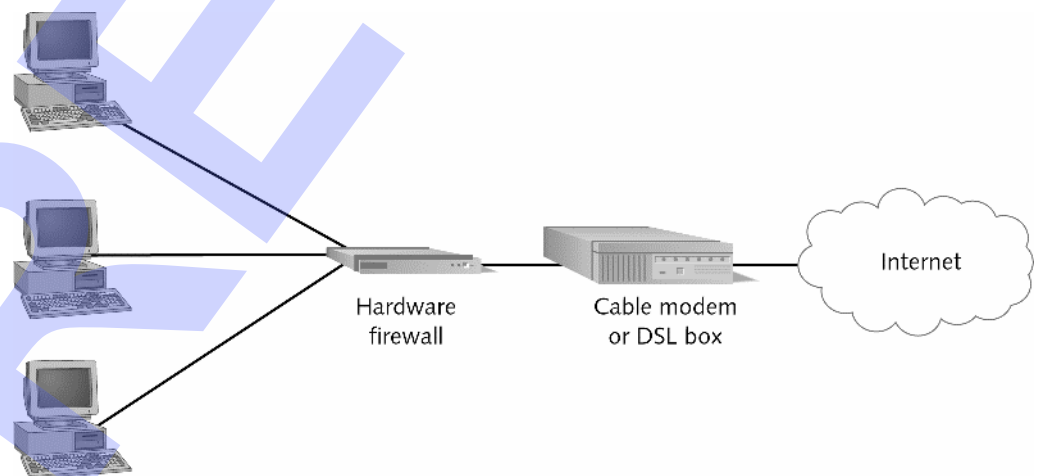


Exhibit 2-18: A hardware firewall

Software firewall

When a home or business computer has an “always on” connection to the Internet, such as a cable modem or DSL, it’s a good idea to install a software firewall in addition to a hardware firewall. Firewall software can be installed on a computer connected directly to the Internet. For a LAN, you can install firewall software on each computer on the LAN. The firewall also requests permission from the user prior to allowing any programs access to the Internet. All open ports are blocked, as are any probes from Web sites.

With Service Pack 2 for Windows XP, Microsoft included the security enhancement Windows Firewall. Unlike most firewalls, Windows Firewall can be configured to block only incoming network traffic on your computer. All outgoing network traffic is allowed to travel, unrestricted, from your computer to its destination. Windows Firewall offers many new features, such as allowing incoming network connections based upon software or services running on a user’s computer and the ability to block network connections based upon its source—the Internet, your LAN, or a specific range of IP addresses. By default, Windows Firewall turns on when Service Pack 2 is installed.

Proxy server

When a proxy server is acting as a firewall, it can filter traffic in both directions. It can filter traffic that’s coming into the network from outside computers, and it can filter traffic that’s leaving the network. One way to filter incoming traffic is to limit communication from the outside to specific ports on the inside of the private network. Some firewalls maintain a list of ports to which they prevent access.

Firewalls filter outgoing traffic through a variety of methods. One method is to examine the IP address of the destination Web site against a list of either allowed addresses or forbidden addresses.

Port and packet filters

When a firewall filters ports, it prevents software on the outside from using certain ports on the network, even though those ports have services listening to them. For example, if you have an intranet Web site that’s to be used only by your employees inside the network, you can set your firewall to filter port 80. Those on the intranet can access your Web server using port 80 as normal, but those outside can’t reach your Web server.

When a router also acts as a firewall, it can be called a screening router. Sometimes, screening routers can use a technique called *stateful inspection*. The router keeps track of all TCP sessions currently made and allows only those packets to pass that have been requested inside the network for these open sessions.

Sometimes, a problem arises when you want to allow certain ports to be accessed but others to be filtered or to allow packets that aren’t a part of a current TCP session, such as when there’s a videoconference. Employees on the inside of your firewall need to participate in a videoconference on the Internet, but when you tell your firewall software to allow these ports needed for the conference to be exposed to the Internet or to allow certain type of packets but not others, sometimes the firewall software doesn’t respond properly. In this case, some system administrators temporarily “drop their shields” and remove port and packet filtering altogether, so the conference can take place. During these times, the network is vulnerable to an attack.

Windows Security Center

A secure computer is more important than ever in protecting against data and identity theft, so Microsoft decided to make it easy for Windows users to manage the most important security settings in one place. Windows Security Center, as shown in Exhibit 2-19, is a new feature added to Windows XP when you install Service Pack 2 (SP2). From this central location, you can manage Windows Firewall, Automatic Updates, and any antivirus software you have installed on the computer. To open Security Center, click Start, choose Control Panel, and click Security Center. (If you're working in Classic View, double-click Security Center in the Control Panel.)



Exhibit 2-19: Security Center in Windows XP

Windows Firewall

Windows Firewall (known as Internet Connection Firewall before SP2) is turned on by default. If a user is experiencing problems sending or receiving data, the problem could be that the current firewall settings are preventing the communication from passing through. You might need to allow a specific type of communication—that's prohibited by default—to pass through the firewall. When you need to configure Windows Firewall, open the Windows Security Center. Under Manage Security Settings For, click Windows Firewall to open the Windows Firewall dialog box, as shown in Exhibit 2-20.

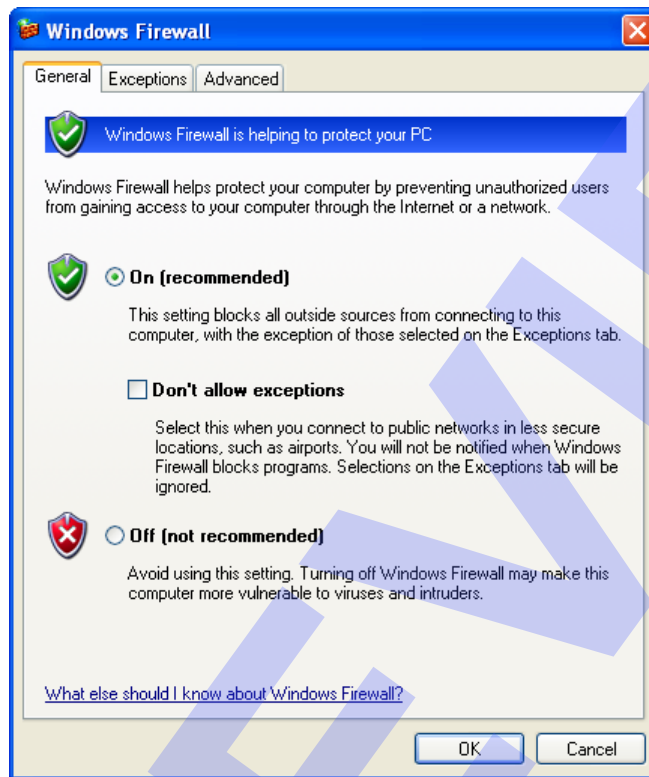


Exhibit 2-20: The Windows Firewall dialog box

You can use this dialog box to turn the firewall on and off, and you can use the Exceptions tab to allow or deny specific types of network communication. The Settings on the Advanced tab let you configure firewall protection for multiple network connections, manage the log file, and configure Internet Control Message Protocol (ICMP) settings. If users are having difficulty accessing Web sites, you should check the firewall settings.

*Do it!***D-1: Configuring Windows Firewall**

Here's how	Here's why
1 Open Control Panel	You're going to configure the firewall to allow communication through Windows Messenger, Microsoft's instant messaging client software.
Click Security Center	To open the Windows Security Center.
2 Under "Manage security settings for," click Windows Firewall	To open the Windows Firewall dialog box.
3 Activate the Exceptions tab	
4 Click Add Program...	
5 Select Windows Messenger and click OK	To add Windows Messenger to the list of exceptions. You'll see that it's been added to the list and the box has been checked.
6 In the Programs and Services list, select File and Printer Sharing	You'll configure specific ports.
7 Click Edit...	
With TCP 139 selected, click Change scope...	
Select My network (subnet) only	To close the port to any traffic that isn't on the subnet.
Click OK	
8 Click OK twice, and close Security Center and Control Panel	

Intrusion detection software

Explanation



Intrusion detection software, sometimes called intrusion prevention software, provides alarms that go off when suspicious activity is spotted. These alarms can be:

- A flashing message to the network administrator
- An e-mail message sent to a specified address
- A pager message

In addition, good intrusion detection software keeps logs of suspicious activities. It also tracks suspicious activity both inside and outside the network. One problem with intrusion detection software is that it might set off an alarm when the activity is harmless. Too many false alarms can cause a user or administrator to ignore a true attack.

Electronic transaction protocols

As the number of companies that sell merchandise over the Internet grows, so does the concern that the transactions aren't secure. New protocols are being developed to help address these concerns and to be certain that all transactions that take place over the Internet are secure. Two of the more popular protocols are SSL (Secure Sockets Layer) and SET (Secure Electronics Transactions).

Secure Sockets Layer

SSL (*Secure Sockets Layer*) is a protocol that was developed by Netscape to provide security between application protocols (such as FTP, HTTP, or Telnet) and TCP/IP. SSL provides data encryption and server authentication, and can provide client authentication for a TCP/IP connection. It's implemented in both Netscape Navigator and Internet Explorer to provide a secure connection when customers are placing orders over the Internet using a browser and a Web site. When you see an address that starts with https://, you know that it's a secure connection.

A browser accessing a secure site uses encryption to scramble information without any interference or knowledge of the user. By default, browsers use a method of encryption that uses a 128-bit key.

SSL uses public and private keys, as shown in Exhibit 2-21.



Use this slide to explain
SSL concepts.

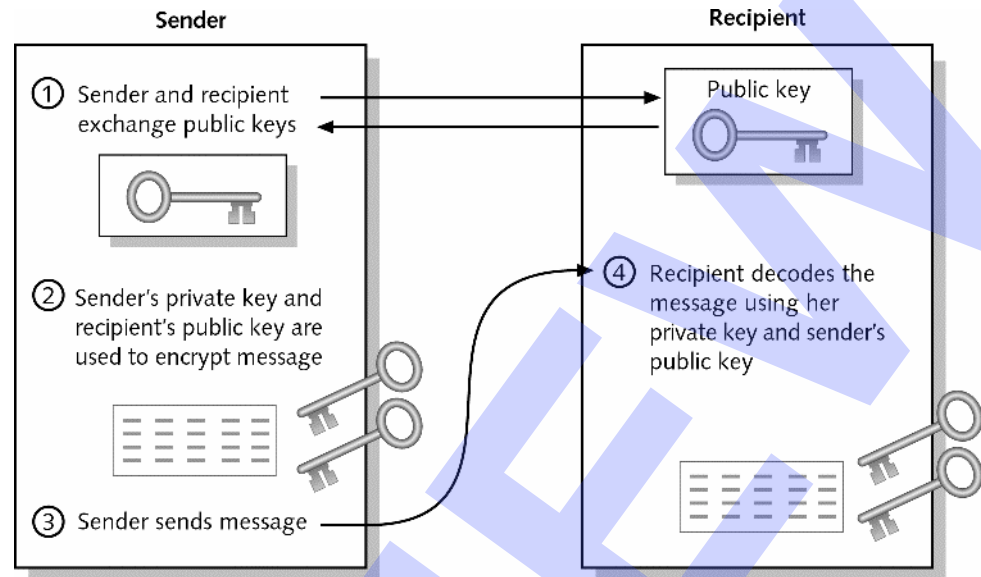


Exhibit 2-21: Using SSL

Secure Electronics Transactions

SET (Secure Electronics Transactions) is a protocol that's designed to offer a secure medium for credit card transactions. It uses digital signatures to verify that both parties involved in the transaction are who they say they are. SET also protects the information in the transaction (including credit card information) from being stolen or altered during the transaction. This feature protects all parties, including the consumer. SET offers an additional protection to consumers by providing a mechanism for their credit card number to be transferred directly to the credit card issuer for verification and billing without the merchant being able to see the number.

When a transaction is made, the customer's browser receives the merchant's public key and the bank's public key, and uses the merchant's certificate to confirm that the merchant is valid. Before the browser sends the order and payment information, information about the purchase is encrypted with the merchant's public key, and the payment information is encrypted with the bank's public key, as illustrated in Exhibit 2-22



Use this slide to explain SET concepts.

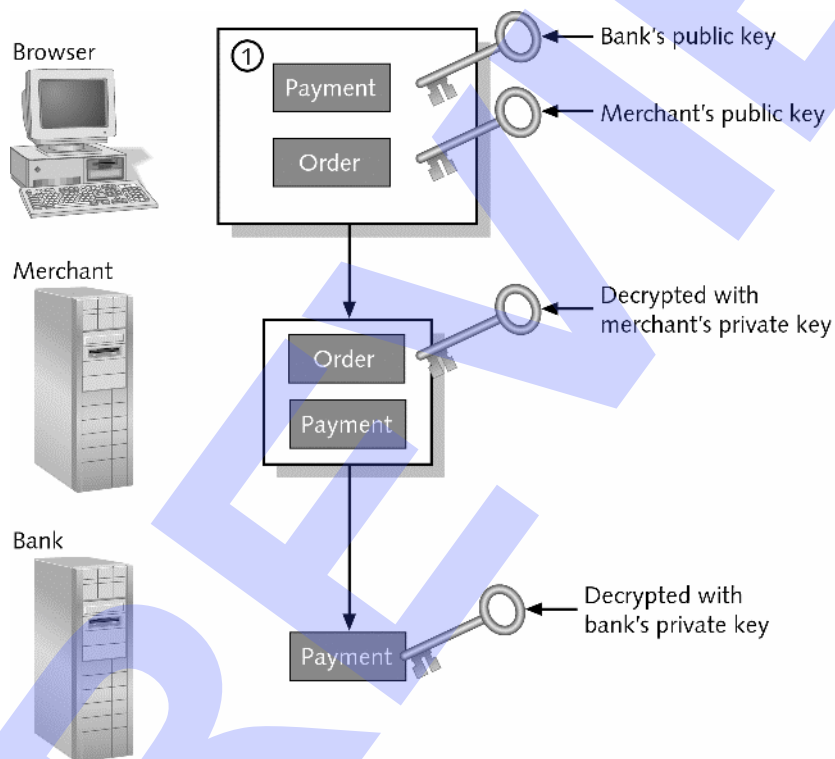


Exhibit 2-22: Using SET security

Antivirus software



To stop viruses and worms, you should install antivirus software on individual computers, servers, and other network devices, such as firewalls. Most antivirus software runs a *real-time antivirus scanner*. A real-time antivirus scanner is software that's designed to scan every file accessed on a computer so that it can catch viruses and worms before they can infect a computer. This software runs each time a computer is turned on. Using a real-time scanner helps antivirus software stop infections from different sources, including a Web browser, e-mail attachment, storage media, or local area network.

Most antivirus software works by using a checksum, a value that is calculated by applying a mathematical formula to data. When the data is transmitted, the checksum is recalculated. If the checksums don't match, the data has been altered, possibly by a virus or worm. The process of calculating and recording checksums to protect against viruses and worms is called *inoculation*.

Definition files

Antivirus software must be updated to stay abreast of new viruses and worms. The software can find only threats that it knows to look for. Therefore, the antivirus software manufacturer constantly provides updates, called virus definitions, to the software as new viruses and worms are discovered. It's important to use antivirus software that automatically checks and updates its virus definitions from the manufacturer's Web site. Having outdated virus definitions is the number one cause of virus or worm infection.

Antivirus products

The following table lists several antivirus software products and their manufacturers' Web sites. Most of these sites offer detailed information about common viruses and worms. They even offer removal tools you can download for free that can be used to remove worms and viruses from infected computers. One of the best ways to protect yourself against viruses and worms is to stay informed. Web sites like www.datafellows.com and www.symantec.com provide descriptions of the latest threats.




Software	Web site address
Norton AntiVirus by Symantec, Inc.	www.symantec.com
Dr. Solomon's Software	www.drsolomon.com
McAfee VirusScan by McAfee Associates, Inc.	www.mcafee.com
ESafe by Aladdin Knowledge Systems, Ltd.	www.esafe.com
F-Prot by FRISK Software International	www.f-prot.com
PC-cillin by Trend Micro (for home use)	www.trendmicro.com
NeaTSuite by Trend Micro (for networks)	
Sybari Antigen	www.sybari.com
avast! by ALWIL Software	www.avast.com

E-mail servers should also have antivirus software installed to protect computers on your LAN. Sybari Antigen (www.sybari.com) is an example of network antivirus software that scans all inbound and outbound e-mail, filters e-mail based on attachment type, and blocks spam.

Do it!

D-2: Installing protection software

Provide students with a copy of avast! or have them download an evaluation copy from www.avast.com.

Here's how	Here's why
1 Install the avast! antivirus software provided by your instructor	(Follow your instructor's directions and the software prompts to install the software.)
2 If prompted to perform a boot time scan of your computer, click Yes	
3 Restart your computer when prompted	The avast! antivirus program scans your local drives.
Click OK	To close the Welcome to avast! Home Edition! dialog box.
4 In the System Tray, right-click  and choose Program Settings...	
5 On the left, select Update (Basic)	To display the options for updating the program and virus database.
6 In the Program section, select Automatic	
7 On the left, select Sounds	(On the left.)
8 Check Disable avast! sounds	
9 Click OK	
10 In the System Tray, right-click  and choose Merge with main avast! icon	To combine the two tray icons into one. VRDB (virus database generation options) will now be available from a submenu when you right-click the main avast! icon.
11 In the System Tray, right-click  and choose Start avast! Antivirus	
In the Registration box, click Demo	After performing a memory scan, avast! displays two windows: a help window and the program's main window.
12 Close the help window	

13 Click where indicated



To select local hard drives as the location to scan.

14 Click where indicated



To begin scanning the selected location (local hard drives) for viruses.

15 Click where indicated



To stop the scan.

16 Close the avast! window

Privacy protection

Explanation



Protecting your privacy includes ensuring that no one is able to gain access to any of your personal information. When you're on the Internet, it's easy for people to find information about you. The information they find might be only your e-mail address, or it might include financial account information. To protect your privacy, you should attempt to:

- Eliminate spam
- Stop pop-up ads
- Remove spyware
- Control cookies

Eliminate spam



To eliminate the amount of spam you receive:

- Complete forms only for Web sites that you trust.
- Uncheck boxes that automatically add you to mailing lists.
- Create a separate e-mail account just for junk mail.
- Don't click on the unsubscribe link in unsolicited e-mail.
- Use your ISP's spam rejection service.
- Complain to the ISP to which the spam originator subscribes.

Stop pop-up ads

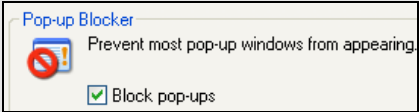


Pop-up ads are additional Web page windows that appear when a user clicks a hyperlink or visits a Web site. A pop-up ad can also contain a hyperlink to a Trojan horse or a virus. Many users accidentally install a Trojan horse while attempting to close pop-up windows.

In Windows XP Service Pack 2, Microsoft added a pop-up blocker to Internet Explorer. When a pop-up is blocked on a Web site, an Information bar appears under the Address bar. If you click the Information bar, you can choose to allow the pop-up, allow all pop-ups from this site, or configure additional settings.

Do it!

D-3: Blocking pop-ups

Here's how	Here's why
<div>1 Open Internet Explorer</div> <div>Choose Tools, Internet Options...</div> <div>2 Activate the Privacy tab</div>	<div></div> <div>By default, Internet Explorer is set to block pop-up ads.</div>

3 Click Settings...

If you frequent Web sites that you want to get pop-up ads from, you can add the individual Web site to this list. For example, Barnes and Noble sometimes uses pop-ups to make you aware of a special promotion or offer a savings coupon code.

In the Address of Web site to allow box, enter
www.barnesandnoble.com

Click **Add**

Click **Close**

Click **OK**

4 Visit www.barnesandnoble.com

It may or may not have current promotions running in a pop-up window.

5 Visit www.cnn.com

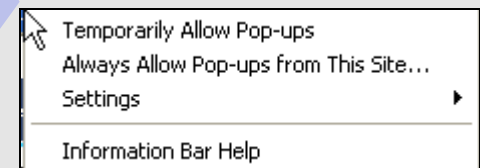
CNN often runs pop-up ads on its site. If there's currently a pop-up ad, Internet Explorer blocks it and displays a message.

If www.cnn.com doesn't have a pop-up, find a site that does.



Click **OK**

To close the Information Bar message box

6 Click the message

You're presented with options.

Observe each of the options

You can temporarily allow pop-ups from this site during this visit. You can add this site to your list of sites that are allowed to display pop-ups, and you can turn off pop-up block temporarily.

7 Choose Temporarily Allow Pop-ups

The CNN pop-up displays.

Close the pop-up ad window

Talk students through each of the options.

Remove spyware

Explanation



Spyware is often secretly installed in addition to normal software that a user installs from the Web. A good pop-up blocker can help reduce the amount of spyware that might be installed on your computer. However, the best recommendation is to minimize or refrain from installing free software from the Web or from peer-to-peer, file-sharing networks.

One of the best programs for removing spyware is called Spybot Search & Destroy (www.safer-networking.org). It can be downloaded at no charge and does a good job of detecting and removing spyware. However, no software is capable of removing all spyware from a computer. You must also update Spybot's spyware definitions before attempting to remove spyware from your computer.

Spyware also integrates itself into Internet Explorer, causing frequent browser crashes. In Windows XP Service Pack 2, Microsoft introduced a feature, called Manage Add-ons, which can be used to view and manage software that has integrated itself into Internet Explorer.

Do it!

D-4: Installing a spyware checker

Here's how	Here's why
1 In Internet Explorer, go to www.safer-networking.org	
Choose your language	
2 Click Download	
3 Next to Spybot – Search & Destroy 1.4, click Download	
Next to any mirror site, click Download here	
Click Download Now	If necessary, click the message to enable Internet Explorer to download the file.
Save the file to your Desktop	
4 When the download is complete, close the Download box and Internet Explorer	
5 On the Desktop, double-click spybotsd14	
Click Run	
Click OK	To accept the default English language.

<p>6 Click Next</p> <p>Select I accept the agreement and click Next</p> <p>Click Next</p> <p>Click Next</p>	<p>To accept the license agreement.</p> <p>To continue with the default installation directory.</p> <p>To continue installing with the default components.</p>
<p>Click Next twice</p> <p>7 Click Install</p> <p>Observe that Run SpybotSD.exe is checked</p> <p>Click Finish</p>	<p>This runs Spybot after the installation finishes.</p>
<p>8 Click OK</p> <p>9 Click Create registry backup</p> <p>When the Registry backup is finished, click Next</p>	<p>To indicate you understand that if you remove advertisement robots with this program, you may not be able to use certain host programs.</p> <p>To back up your Registry before running Spybot and removing any items.</p>
<p>10 Click Search for updates</p> <p>Click Download all available updates</p>	<p>Like a virus scanning program, Spybot adds items to its watch list (called detection rules) often. You need to update this list on your copy of Spybot.</p>
<p>11 Click OK</p> <p>Click Immunize</p> <p>Click OK</p>	<p>To indicate you understand that if you remove advertisement robots with this program, you may not be able to use certain host programs.</p> <p>To close the Warning box.</p>

12 Click **Search & Destroy**

Click **Check for problems**

If any problems are found, click **Fix selected problems** and click **Yes**, then **OK**

13 Close Spybot – Search & Destroy

This area of the Spybot program allows you to scan for problems and remove them.


Problem

 **Congratulations!**
No immediate threats were found.

If your computer did have problems, they'd be listed in the Problem box. You could select the ones you wanted to delete.


Control cookies

Explanation



One step in protecting your privacy is to limit the cookies that you allow to be placed on your computer. Internet Explorer users can control cookies through the Privacy tab of the Internet Options dialog box. Using this option, you can configure Internet Explorer to reject all cookies. Unfortunately, many Web sites rely so heavily on cookies that you'll have problems using those sites if you don't allow your browser to accept cookies. You might not be able to access some sites at all unless you have cookies enabled.

Do it! D-5: Controlling cookies

Here's how	Here's why
<p>1 Open Internet Explorer</p> <p>Choose Tools, Internet Options...</p> <p>Activate the Privacy tab</p> <p>2 Under Settings, move the slider to High</p> <p>3 Click Sites...</p>	<div><p>High</p><p> - Blocks cookies that do not have a compact privacy policy - Blocks cookies that use personally identifiable information without your explicit consent</p></div> <p>This security setting blocks cookies from sites that don't have a compact privacy policy or that use personally identifiable information with your explicit consent.</p> <p>You can add sites that are explicitly allowed to put cookies on your computer or blocked from putting cookies on your computer, regardless of whether or not they meet the security level you set (in this case High).</p>

- 4 In the Address of Web site box, enter **www.ebay.com** and click **Block**

In the Address of Web site box, enter **www.cnn.com** and click **Allow**

Click **OK** twice

- 5 Go to **www.ebay.com**

To block this Web site from placing cookies on your computer, regardless of its privacy policy.

To allow this Web site to place cookies on your computer, regardless of its privacy policy.




Your privacy policy blocked a cookie from **www.ebay.com** from being placed on your computer.

Click **OK**

If there's no cookie, try another Web site.

- 6 Go to **www.cnn.com**

Notice your privacy policy blocks a cookie

 appears in the status bar.

- 7 Double-click 

Web sites with content on the current page:	
Site	Cookies
http://servedby.advertising.com/site=695349/size=72809...	Blocked

To open the privacy report. The cookie that was blocked was not from **www.cnn.com**. It was from an advertising company.

- 8 Click **Close** and close Internet Explorer

Web browsers

Explanation



Most people associate Web browsers with leisure-time entertainment, but many users require Internet access at their workplace so they can perform research and access information both from the Internet and from an intranet. An *intranet* is an internal, company-owned, Internet-like network maintained for the benefit of employees. You can also set up an intranet within your home for the benefit of everyone living there.

Web browsers are widely used, so they're often the target of hackers, who use vulnerabilities in the browser's code to wreak havoc and steal data. Preserving the security of your computer when you browse the Web is a balancing act. The more open you are to downloads of software and other content, the greater your exposure to risk. For example, you want to avoid the risk of downloading software that could damage data on your hard drive, but the more restrictive your settings, the less useful the Web becomes.

The following discussion focuses on Internet Explorer, the most widely used browser in the world. Other browsers have similar security settings. You'll need to investigate the security settings in other browsers if you need to configure them.

The following discussion focuses on Internet Explorer 6. At this point in time, users shouldn't have any other version of Internet Explorer installed for a variety of reasons, most important being the potential security risks.

Installing Internet Explorer

Internet Explorer is installed by default in all Microsoft operating systems. It is a Windows Component and you can uninstall and reinstall it in Control Panel by using the Add/Remove Windows Component feature of Add or Remove Programs. If Internet Explorer is checked, it is installed.

Internet Explorer security zones

Security zones offer a method for managing a secure Web environment. You can use security zones to implement your organization's Internet security policies by grouping sets of sites together and assigning a security level to each zone. Exhibit 2-23 shows the security zones in Windows XP.



Use this slide to explain security zone concepts.

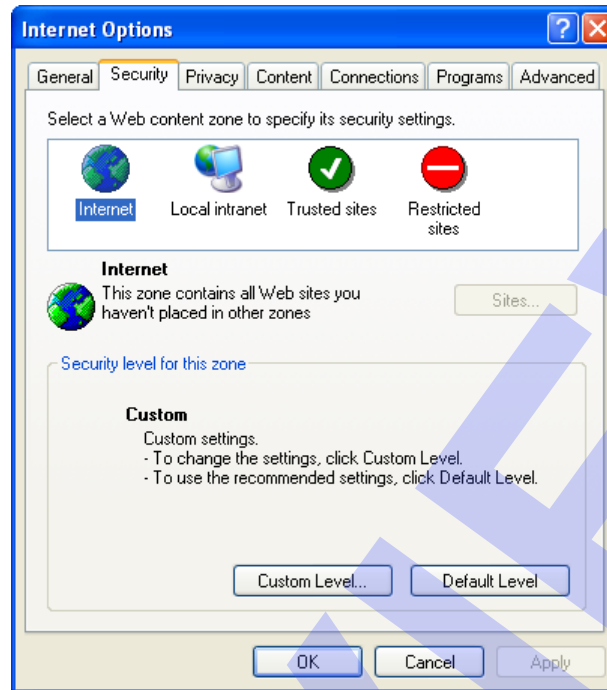


Exhibit 2-23: Internet Explorer security zones

A *security zone* is a group of Web sites that can be separated in order to manage security. When you first install Internet Explorer 6, it groups all Web sites into a single zone, called the Internet zone, which applies a medium level of security. This allows users to browse Web sites securely, but it prompts users before they download potentially unsafe content.

Internet Explorer includes the following Security zones:

- **Internet zone** — The Internet zone consists of all Web sites that are not included in the other security zones. This zone is set to the Medium security level by default. If your organization is concerned about possible security problems when users browse the Web, you can change the Internet zone's security level to High. This change might cause some pages to malfunction or be displayed incorrectly. You can also consider specifying a Custom security level that permits controlling each security decision for the zone.
- **Local intranet zone** — The Local intranet zone includes Web sites on an organization's intranet. You set up the Local intranet zone in conjunction with your firewall. All sites in this zone should be inside the firewall. Obtain detailed information about your internal network from the network administrators. This zone consists of local domain names by default.
- **Trusted sites zone** — The Trusted sites zone includes Internet sites you have designated as trusted. These sites can include the Web sites of business partners or reliable public entities. The Trusted zone is assigned the Low security level by default. The Web site will be allowed to perform a wider range of actions. This zone is intended for highly trusted Web sites only.

- **Restricted sites zone** — The restricted sites zone includes all sites that you do not trust. When you assign a Web site to the Restricted sites zone, it will be allowed to perform only minimal, very safe actions. This zone is set to the High security level by default. The High security level might cause Web pages to malfunction or be displayed incorrectly.

The following table describes the security levels you can set for each security zone.

Level	Safeguards	Content	Appropriate zone
Low	Minimal safeguards and warning prompts	Most content is downloadable and runs	Trusted sites
Medium-Low	Minimal safeguards and warning prompts	Most content is downloadable and runs	Local intranet
Medium	Safe browsing and still functional	Prompts before downloading potentially unsafe content	Internet
High	Safest, yet least functional	Less secure features are disabled	Untrusted sites

The Security Settings dialog box

Clicking the Custom Level button on the Security tab opens the Security Settings dialog box, shown in Exhibit 2-24. At the top of the dialog box is the Settings list box. You can use this to enable or disable the specific security options (including script support), depending on the security policies established by your organization. The custom level options are grouped into the following categories:

- **ActiveX controls** — Approves, downloads, runs scripts with ActiveX controls (software components designed to interact with one another in a networked environment). Use these settings to enable/disable script support.
- **Downloads** — Allows file or font downloads.
- **Scripting** — Allows scripts to be run.
- **User authentication** — Specifies the method needed to log on to a Web site.
- **Miscellaneous** — Permits or restricts a wide range of actions.

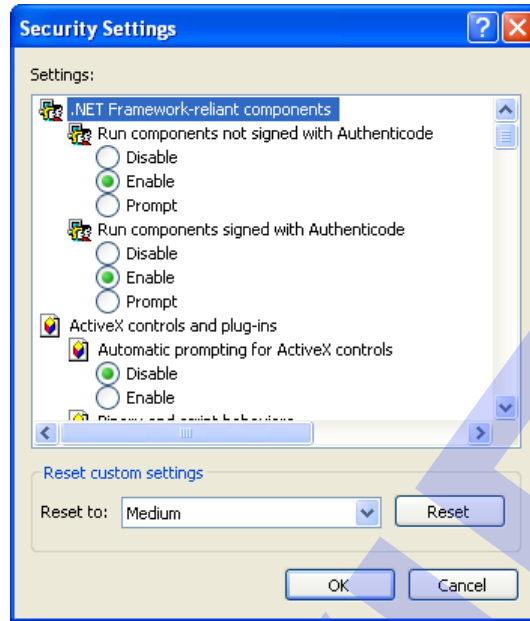


Exhibit 2-24: Internet Explorer security settings

Microsoft provides client-side software that watches for the downloading of supported software such as ActiveX controls and executable files. If a piece of software has been digitally signed, Internet Explorer can verify that the software originated from the developer and that no one has tampered with the software. A valid digital signature does not guarantee that the software is without problems; it means that the software has not been modified. Likewise, software without a signature does not prove that the software is dangerous; however, it does alert the user to potential problems.

Do it!

D-6: Setting security zones

The Internet Options dialog box is open.

Here's how

- 1 Open Internet Explorer

Choose **Tools, Internet Options...**

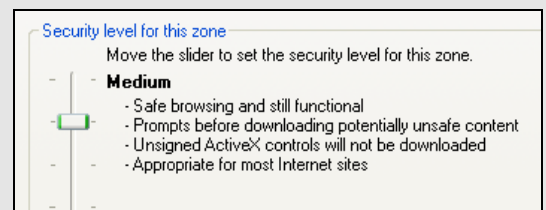
Activate the Security tab

- 2 With Internet selected, click **Default Level**

Here's why

You're going to configure Internet Explorer security zones, one of the methods used to control security in this popular browser.

To open the Internet Options dialog box.



The default security level for the Internet security zone is Medium.

3 Click **Custom Level...**

To open the Security Setting dialog box.

Scroll the Settings box and observe the security settings for the Medium security level

Click **Cancel**

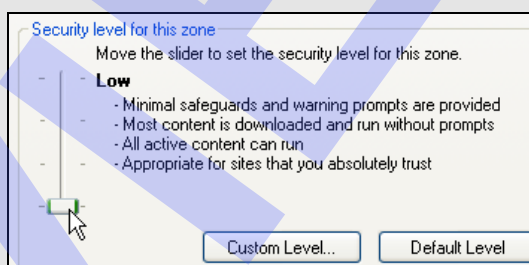
To return to the Internet Options dialog box.

4 Select **Local intranet**



5 Click **Default Level**

Drag the slider to **Low**



6 Select **Trusted sites**

Click **Sites...**

7 Clear **Require server verification (https:) for all sites in this zone**

8 In the “Add this Web site to the zone” box, type **www.microsoft.com**

Click **Add**

To add Microsoft’s Web site to the Trusted sites zone.

Click **OK**

9 Click **Default Level**

To verify that the Trusted sites zone is set to Low.

10 Select **Restricted sites**

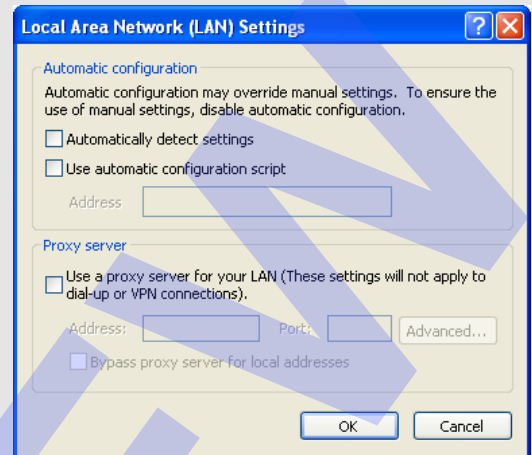
Click **Default level**

To verify that the Restricted sites zone is set to High.

11 Click **Apply**

To apply the settings on the Security tab of the Internet Options dialog box.

- 12 Activate the Connections tab and click **LAN Settings...**



You'd use this dialog box to configure proxy server settings.

- 13 Click **Cancel** and click **OK**

Close Internet Explorer

Wireless standards

Explanation



Ever since the first wireless transmissions took place over a century ago, there has been a push to manage the public airwaves responsibly. During that time, frequency bands have been divided up to accommodate the various user categories such as the military, broadcasters, and amateur radio operators. One of the issues with the current wireless technology is that it's a broadcast signal. This means a wireless device advertises its presence, making it easy for an intruder to pick up and monitor. In order to prevent this from happening, standards were developed and implemented. The WLAN solution provided by Windows XP and Windows Server 2003 is based on IEEE standards 802.1x and 802.11.

802.1x standard

The *802.1x standard* is a port-based, authentication framework for access to Ethernet networks. Although this standard is designed for wired Ethernet networks, it applies to 802.11 WLANs. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. It requires three roles in the authentication process:

- A device requesting access
- An authenticator
- An authentication server

802.1x allows scalability in wireless LANs by incorporating centralized authentication of wireless users or stations. The standard allows multiple authentication algorithms and is an open standard.

802.11 standard

The IEEE 802.11 standard specifies a technology that operates in the 2.4 through 2.5GHz band. Wireless networks operate according to the specifications of the IEEE 802.11 standards. The IEEE 802.11 standards are defined at the Data Link layer of the Open Systems Interconnection (OSI) model. In this standard, there are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network on the fly. The 802.11 standard also places specifications on the parameters of both the physical and medium access control (MAC) layers of the network.

The 802.11 standard defines an *access point (AP)* as a device that functions as a transparent bridge between the wireless clients and the existing wired network. The access point contains at least one interface to connect to the existing wired network and transmitting equipment to connect with the wireless clients. It also contains IEEE 802.1D bridging software, to act as a bridge between wireless and wired data-link layers. The current and future WLAN standards under 802.11 are described in the following table.

Standard	Description
802.11a	Ratified in 1999, 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM). OFDM offers significant performance benefits compared with the more traditional spread-spectrum systems. OFDM is a modulation technique for transmitting large amounts of digital data over radio waves. Capacity per channel is 54 Mbps with real throughput at about 31 Mbps. It operates at a frequency of 5 GHz, which supports eight overlapping channels.
802.11b	Ratified in 1999, 802.11b is one of the most popularly used 802.1x technologies. Uses Direct Sequence Spread Spectrum (DSSS). Capacity per channel is 11 Mbps with real throughput at about 6 Mbps. It operates at a frequency of 2.4 GHz, which supports three non-overlapping channels.
802.11c	Pertains to the operation of bridge connections. Was moved to the 802.1 standards set.
802.11d	Ratified in 2001, 802.11d aims to produce versions of 802.11b that are compatible with other frequencies so it can be used in countries where the 2.4 GHz band isn't available.
802.11e	Not yet ratified, 802.11e will add Quality of Service (QoS) capabilities to 802.11 networks. It uses a Time Division Multiple Access (TDMA) scheme and adds extra error correction.
802.11f	Ratified in 2003, 802.11f improves the handover mechanism in 802.11, so that users can maintain a connection while roaming. It's aimed at giving network users the same roaming freedom that cell phone users have.
802.11g	Ratified in 2003, 802.11g is a combination of 802.11a and 802.11b. It can use either Direct Sequence Spread Spectrum (DSSS) or Orthogonal Frequency Division Multiplexing (OFDM). Capacity per channel is 54 Mbps with real throughput at about 12 Mbps. It operates at a frequency of 2.4 GHz. 802.11g is also a popularly used 802.11 technology.
802.11h	Ratified in 2003, 802.11h attempts to improve on 802.11a by adding better control over radio channel selection and transmission power.

Standard	Description
802.11i	Ratified in 2004, 802.11i deals with security. This is an entirely new standard based on the Advanced Encryption Standard (AES). This standard has a feature called Robust Security Network (RSN), which defines two security methodologies. The first is for legacy-based hardware using RC4, and the second one is for new hardware based on AES. WPA implemented a portion of this standard. WPA2 implements the entire standard. 802.11i is also known as WPA2.
802.11j	Ratified in 2004, 802.11j allows 802.11a and HiperLAN2 networks to coexist in the same airwaves. 802.11j made changes to the 5GHz signaling capabilities to support Japan regulatory requirements.
802.11k	A WLAN management system, currently in progress.
802.11l	This letter was skipped by the IEEE governing board to avoid confusion with 802.11i.
802.11m	This contains maintenance of the 802.11 family documentation.
802.11n	Currently in progress, 802.11n is a 100+ Mbps standard.

While devices that support the 802.11a standard are generally incompatible with those that support 802.11b, some devices are equipped to support either 802.11a or 802.11b. The newest standard, 802.11g, allows 802.11b and 802.11g devices to operate together on the same network. This standard was created specifically for backwards compatibility with the 802.11b standard.

WLAN security

Given all of the benefits, the security drawbacks with WLANs would need to be fairly severe to undermine their appeal. Wireless devices present a whole new set of threats that network administrators are unaware of. The most obvious risks concerning wireless networks are theft and rogue devices. Most cell phones, text pagers, PDAs, and wireless network cards are small enough that they can be easily lost or stolen. Because they're simple to conceal and contain valuable information about a company, they've become favorite targets of intruders. Wireless LANs can be subject to session hijacking and man-in-the-middle attacks. Additional risks remain, because anyone can purchase an access point and set it up.

WLAN security problems

Wireless access points, when set up right out of the box, have no security configured. They broadcast their presence—in essence saying, "Hey, my name is xxx, here I am!" The free availability of 802.11 network audit tools, such as AirSnort and NetStumbler, means that breaking into wireless networks configured with weak security is quite easy. These tools can be used to check wireless security by identifying unauthorized clients or access points, as well as verifying encryption usage. There are tools available in the form of management software. To eliminate existing 802.11 shortcomings and to help improve the image of wireless technology on the market, the *Institute of Electronic and Electric Engineers (IEEE)*, together with the *Wireless Ethernet Compatibility Alliance (WECA)*, proposed standards for significantly improved user authentication and media access control mechanisms.

Additional risks associated with wireless networks include:

- 802.1x transmissions generate detectable radio-frequency traffic in all directions. Persons wishing to intercept the data transmitted over the network might use many solutions to increase the distance over which detection is possible, including the use of metal tubes such as a Pringles container or a large tomato juice can.
- Without the use of an encryption standard of some type, data is passed in clear text form. Even though technologies, such as Wired Equivalent Privacy (WEP), encrypt the data, they still lack good security, and a determined listener can easily obtain enough traffic data in order to calculate the encryption key in use.
- The authentication mechanism is one-way, so it's easy for an intruder to wait until authentication is completed and then generate a signal to the client that tricks the client into thinking that it has been disconnected from the access point. Meanwhile, the intruder begins to send data traffic to the server pretending to be the original client.
- The client connection request is a one-way open broadcast. This gives an intruder the opportunity to act as an access point to the client and act as a client to the real network access point. This allows an intruder to watch all data transactions between the client and access point, then modify, insert, or delete packets at will.
- A popular pastime is wardriving. *Wardriving* involves driving around with a laptop system configured to listen for open wireless access points. Several Web sites provide detailed information locating unsecured networks. These sites provide locations, sometimes on city maps for the convenience of others looking for open access links to the Internet. This is an attractive method not to only capture data from networks, but also to connect to someone else's network, use their bandwidth, and pay nothing for it.
- *War chalking* is the process of marking buildings, curbs, and other landmarks indicating the presence of an available access point and its connection details by utilizing a set of symbols and shorthand.

WLAN security solutions

Wireless security comes in two major varieties today:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)

Both include methods to encrypt wireless traffic between wireless clients and APs. WEP has been included in 802.11-based products for some time and includes a strategy for restricting network access and encrypting network traffic based upon a shared key. A company can protect itself from security threats by:

- Enabling WEP—Nearly all Wi-Fi certified products ship with basic encryption capabilities (40-bit key WEP). However, it isn't enabled by default. When you enable WEP, it's designed to provide the same level of security as your wired LAN.
- Changing default access point administration passwords—Many devices right out of the box don't have a password set on the Administrator account. Programs, such as AirSnort, identify the manufacturer based on the MAC address, so if you change only the SSID, chances are that an informed hacker can easily gain access.



- Changing default Service Set Identifiers (SSIDs)—Don't change the SSID to reflect your company's main names, divisions, products, or address. This makes you an easy target. If a SSID name is enticing enough, it might attract hackers.
- Disabling broadcast SSID—Broadcast SSID is enabled by default. This means it will accept any SSID. When you disable this feature, the SSID configured in the client must match the SSID of the access point.
- Separating the wireless network from the wired network—Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points. The wireless clients can be separated so the connections not only use RADIUS authentication but are also logged.
- Putting the wireless network in an Internet access-only zone or a Demilitarized Zone (DMZ)—Place your wireless access points in a DMZ and have your wireless users tunnel into your network using a VPN. This requires extra effort on your part to set up a VLAN for your DMZ, but this solution adds a layer of encryption and authentication that makes your wireless network secure enough for sensitive data.
- Disabling DHCP within the WLAN to keep a tighter control over users—Assign static IP addresses to your wireless clients. This creates more administrative overhead to manage, but it makes it harder to access your network.
- Enabling MAC address filtering on access points to limit unauthorized wireless NICs—Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of the wireless client's NIC isn't in the access point's table, access is denied. Although there are ways of spoofing a MAC address, it takes an additional level of sophistication.

You should consider periodically surveying your site using a tool, such as NetStumbler or AirSnort, to see if any rogue access points are installed on the network. You should also determine if there are any unused wireless connections and remove or disable them. In addition, take a notebook equipped with a wireless sniffer installed and an external antenna outside your office building. Check to see what information inside your building can be accessed by someone parked in the parking lot or across the street.

Frequency management

Wireless network signals are sent and received via radio signals associated to a specific access point and a wireless network card. In the USA, 802.11b and 802.11g networks can use channels 1, 6, and 11. There are eleven channels available, but by the time you account for 22 MHz separate between the channels, that leaves you with only those three channels. 802.11a improves on this availability by providing eight channels. This gives network administrators more flexibility in assigning channels.

Two access points that use the same channel result in signal overlap. This will result in interference and will confuse the wireless cards within the area of the overlap.

To help secure your wireless network, you should plan frequency management so that the signal doesn't reach beyond where you want people to be able to access your wireless network. For example, if you don't want people in the house across the street from being able to access your network, then frequency management is one of the steps you can take to help limit access to your network.

Other objects that operate on the 2.4 or 5 GHz band such as microwave ovens, cordless phones, and cameras can interfere with the wireless network signal. Be aware of this when planning your network as well as when you are troubleshooting access problems.

Do it!

D-7: Identifying the technology used to implement WLANs**Questions and answers**

- 1 You work for a company that supplies parts to several automobile dealerships on a daily basis. Each part is assigned an ID, and that ID is bar coded on the shelf where it's stocked. Currently, as each item is pulled for delivery, it's taken to one of the three central computers and scanned to update the inventory database. Can wireless networking benefit your organization?

Yes, implementing wireless networking would allow personnel to scan the bar code on the shelf with a handheld wireless device, as each item is pulled from stock. One of the benefits of wireless networking is that inventory taking is more convenient, because personnel can freely walk around the warehouse or organization.

- 2 Match the 802.11 standard with its description.

A. 802.11a

D. It can use either DSSS or OFDM and operates at a frequency of 2.4 GHz.

B. 802.11b

B. Uses Direct Sequence Spread Spectrum (DSSS) operating at a frequency of 2.4 GHz, which supports three non-overlapping channels.

C. 802.11F

D. 802.11g

A. Uses the OFDM modulation technique for transmitting large amounts of digital data over radio waves. It operates at a frequency of 5 GHz, which supports eight overlapping channels.

E. 802.11i

E. A standard based on the Advanced Encryption Standard (AES). It includes a feature called Robust Security Network (RSN), which defines two security methodologies: the first is for legacy-based hardware using RC4, and the second one is for new hardware based on AES.

C. Allows users to maintain a connection while roaming.

- 3 What are the two technologies you can use to secure your wireless networks?

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA)

- 4 You've recently been hired as a consultant to evaluate Outlander Spices wireless network security. What items should you check in evaluating their security practices?
- *Is WEP enabled on their wireless devices? If not, enable WEP.*
 - *Have they changed the default administrator passwords on their wireless access points? If not, change the default administrative passwords on the devices using a complex password.*
 - *Are they still using the default Service Set Identifiers (SSIDs) on their WAPs? If they are, change the SSIDs, but don't use meaningful names, such as division or department names.*
 - *Are they still broadcasting SSIDs? If so, disable broadcast SSID, so the client SSID and the WAP SSID match.*
 - *Are they using RADIUS to add authentication to their WAP? If not, consider setting up a RADIUS server to authenticate the wireless connections with the WAP.*
 - *Is the wireless network in a DMZ? If not, consider setting up an Internet-only zone and placing the wireless network in it to add a layer of encryption and authentication that makes the wireless network secure enough for sensitive data.*
 - *Are wireless clients getting their IP addresses assigned statically or dynamically from a DHCP server? If the wireless clients are using DHCP, change to static IP addresses for wireless clients.*
 - *Are MAC filters in place? If not, enable MAC address filtering on access points to prevent unauthorized wireless NICs from accessing the network.*

Wireless access point configuration

Explanation



After you've installed your wireless access point, you need to configure it. To configure your wireless access point properly for secure connections, you should:

- Enable WEP
- Alter the wireless access point's factory settings
- Use MAC filters
- Enable 802.1x
- Use Wi-Fi Protected Access mode

Enabling WEP

WEP encrypts data across the wireless network using a network key that can be automatically provided for clients. WEP encryption uses a shared-secret key and the RC4 encryption algorithm. The access point (AP), and all stations that connect to it, must use the same shared key. For each packet of data sent in either direction, the transmitter combines the contents of the packet with a checksum of the packet. Once you've created a wireless network policy in Group Policy, you can configure WEP to enable:

- Data encryption (WEP-enabled)
- Network authentication (Shared mode)
- Provide the key automatically

If available, use 128-bit WEP and change the keys frequently. The WEP standard doesn't provide for any way to change keys automatically. As a result, you can only rekey an AP and its stations manually, unless the access points can provide dynamic WEP keys, and wireless clients can support dynamic WEP keys.

Alter wireless access point factory settings

In addition to enabling WEP on the wireless access point, you should also change the WAP's default settings. WAPs broadcast their Service Set Identifier (SSID)—the name designated for a specific wireless LAN by default. The SSID's factory setting is usually DEFAULT, and it typically doesn't have a password set on the Administrator account. Changing the default SSID helps protect your network. Leaving the default SSID and password on WAP is like using admin and password for the login and password on a server. You can easily change a WAP's SSID to connect to an existing wireless network or to establish a new wireless network.

Use MAC filters

You can also use MAC filters to allow or deny computers access to the network based on their MAC addresses. Enabling MAC address filtering on access points limits unauthorized wireless NICs. Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of the NIC isn't in the table of the access point, it won't allow access.

Enable 802.1x

802.1x is the recommended method of authentication and encryption for enhanced security on computers running Windows XP and Windows Server 2003. The use of 802.1x offers an effective solution for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties EAP to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. You configure 802.1x encryption from the IEEE 802.1x tab of the policy setting's Properties dialog box.

Use Wi-Fi Protected Access

Most WAPs have a configuration mode of *Wi-Fi Protected Access (WPA)*. WPA authorizes and identifies users based on a secret key that changes automatically at a regular interval. WPA uses TKIP (Temporal Key Integrity Protocol) to change the temporal key every 10,000 packets. This ensures much greater security than the standard WEP.

Finally, don't forget to remove any unused wireless connections (access points). These just provide another way for an intruder to access your network resources without your knowledge.

Do it!

D-8: Configuring a wireless access point (instructor demo)

You need a wireless access point installed on your classroom network to complete this activity. The steps were written for a D-Link WAP. If your WAP is different, alter the steps accordingly.

You also need your computer's MAC address.

Here's how	Here's why
1 Open Internet Explorer and enter the IP address of your WAP	You're prompted for administrator credentials on the WAP.
2 Enter the appropriate username and password for your WAP and click OK	
3 Activate the Wireless Settings tab	
In the SSID box, edit default to read warehouse	WEP key: _____
For SSID broadcast, select Disabled	
For Security, select WEP and record the WEP key	
Check Apply	The device restarts itself.
4 Activate the Tools tab	
In the New password and Confirm password boxes, enter !pass4321	
Check Apply	
5 Activate the Advanced tab	
Select MAC filters	
Choose Only allow computers with MAC address listed below to access the network	
In the Name box enter your computer's name	
In the MAC address box, enter your computer's MAC address	
Check Apply	
6 Close Internet Explorer	

Let students know that they'd continue to add MAC addresses for all computers to which they want to allow access to the WAP.

Wireless clients

Explanation

The wireless client must submit its credentials with the authenticating server before wireless network access is established. When the client computer is in range of the WAP, it tries to connect to the WLAN that's active on the WAP. If the WAP is configured to allow only secured or 802.1x-authenticated connections, the WAP issues a challenge to the client. The WAP then sets up a restricted channel that allows the client to communicate only with the RADIUS server. The RADIUS server accepts a connection only from a trusted WAP or from one that has been configured as a RADIUS client on the Microsoft Internet Authentication Service (IAS) server and provides the shared secret for that RADIUS client. The RADIUS server validates the client credentials against the directory. If the client is successfully authenticated, the RADIUS server decides whether to authorize the client to use the WLAN. If the client is granted access, the RADIUS server transmits the client master key to the WAP. The client and WAP now share common key information that they can use to encrypt and decrypt the WLAN traffic passing between them. How you configure Windows clients to participate in this process depends on the operating system.

Windows XP wireless clients

Wireless Auto Configuration dynamically selects the wireless network to which a connection attempt is made, based on configured preferences or default settings. Computers running Windows XP support Wireless Zero Configuration, which enables computers to connect automatically to available wireless networks. Windows XP client computers can choose from available wireless networks and connect automatically, by default, without user action. Wireless Zero Configuration automatically configures items, such as TCP/IP settings, DNS server addresses, and IAS server addresses. Wireless Zero Configuration includes support for 802.1x authentication and encryption. The default preferences for Wireless Zero Configuration using IEEE 802.1x authentication include:

- Infrastructure before ad hoc mode and computer authentication before user authentication.
- WEP authentication attempts to perform an IEEE 802.11 shared key authentication if the network adapter has been preconfigured with a WEP shared key; otherwise the network adapter reverts to the open system authentication.

Although the IEEE 802.1x security enhancements are available in Windows XP Professional, the network adapters and access points must also be compatible with this standard for deployment.

You can change the default settings to allow guest access, which isn't enabled by default. You shouldn't turn on guest access on a laptop using Wireless Zero Configuration. An unauthorized user could establish an ad hoc connection to the laptop and gain access to confidential information on it.



Windows 2000 wireless clients

Computers running Windows 2000 don't support Wireless Zero Configuration. You can configure a wireless network card for connection, using EAP-TLS or PEAP authentication, just as you can when configuring Windows XP computers. Only Windows XP computers natively support IEEE 802.1x authentication. Microsoft provides an 802.1x Authentication Client download that allows Windows 2000 computers to use the 802.1x standard. This download can be found at www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp. Microsoft also provides 802.1x Authentication Clients for Windows 98 and Windows NT 4.0 Workstation to customers with Premier and Alliance support contracts.



Windows CE wireless clients

Palm-top computers running Windows CE .NET include Wireless Zero Configuration and similar manual configuration options to those found on Windows XP. They support 802.11a and Native Wireless Fidelity (Wi-Fi). You can configure older Windows CE palm-top computers for wireless networking. The settings and configuration are similar to those for Windows 2000.

With the differences in configuration and the ability to use Wireless Zero Configuration, when you configure client policies, place Windows XP computers into a separate OU. Define policies that apply only to these computers in a GPO linked to this OU and policies that apply to Windows 2000 computers in a GPO linked to the OU in which these computers are located.

Do it!

D-9: Configuring a wireless client (instructor demo)



Your WAP is set to allow your computer access as directed in the previous activity.

Here's how	Here's why
<ol style="list-style-type: none"> Click Start and choose Control Panel, Network and Network Connections, Wireless Network Connection Click Properties Activate the Wireless Networks tab Under Preferred Networks, click Add... In the SSID box, enter warehouse Check Data Encryption (WEP enabled) Click OK twice Click Close 	<p>You'll configure the client to connect using the settings on the wireless access point.</p>

Unit summary: Computer networking

- Topic A** In this topic, you learned how to configure a LAN connection. You learned about the various **networking models** and the computer roles in each. You installed a **network interface card** and configured it to communicate using **TCP/IP**. You joined a **Windows workgroup** and learned how to view resources on the network.
- Topic B** In this topic, you learned how to **share resources**. First you shared files and folders, and then accessed them from another computer. Then you shared and accessed printers on a network.
- Topic C** In this topic, you learned how to create an **Internet connection**. You identified the various connection technologies available and their appropriate uses. You also discussed the various **WAN bandwidth technologies**.
- Topic D** In this topic, you learned how to configure **Windows Firewall** and secure your wireless network.

Review questions

- 1 Which networking model requires that each individual user has an account on all computers he or she wishes to access shared resources on?
Peer-to-peer networking model
- 2 What's the Windows 2000/2003 Server feature that uses a hierarchical organization to provide an administrator with a single place for all system administration, including user and computer configuration and management; follows the client/server model; and allows users to access network resources from any computer on the network?
The Active Directory
- 3 Which is the service that translates computer names, called host names, into IP addresses on a LAN and on the Internet?
 - A DHCP
 - B DNS**
 - C WINS
 - D Active Directory
- 4 Which is the built-in identifying address coded into a NIC by the manufacturer?
 - A IP address
 - B Subnet mask
 - C MAC address**
 - D I/O address

5 Which communication protocol isn't routable?

- A TCP/IP
- B IPX/SPX
- C AppleTalk
- D NetBEUI**

6 What are the two components of an IP address?

Part of the IP address defines the network address, also known as the subnet; the other part defines the computer address.

7 What are the two components of a DNS name?

DNS host names include a NetBIOS-type computer name plus the DNS suffix of the DNS domain of which the computer is a member.

8 What are the three settings that IPX/SPX (NWLink) requires?

An external network number, an internal network number, and a frame type

9 If a user can't share files and folders, which client software is probably not installed on their computer?

File and Printer Sharing for Microsoft Networks

10 A user can't assign NTFS permissions in addition to the share permissions he or she has assigned to a shared folder. What do you suspect is the problem?

The drive where the shared folder is located is formatted to FAT or FAT32, not NTFS.

11 What's the Universal Naming Convention (UNC) format for connecting to a share?

The format for the UNC is \\computername\sharename.

12 What's the protocol used to send e-mail to an e mail server?

- A POP
- B IMAP
- C SMTP**
- D HTTPS

13 Which is a public-key/private-key encryption protocol used to transmit data securely across the Internet over TCP/IP?

- A SSL**
- B HTTP
- C HTTP-S
- D Telnet

- 14 Which is a fast data transmission technology, affordable for home use, offers a direct connection rather than a dial-up connection, and is a broadband technology that uses ordinary copper telephone lines and a range of frequencies on the copper wire that aren't used by voice, making it possible for you to use the same telephone line for voice and data at the same time?

A PPPoE
B ISDN
C DSL
D Bluetooth

- 15 What are the components necessary to create a valid network connection through the LAN to the Internet?

At a minimum:

- A working network card
- An IP address
- A subnet mask
- The IP address of a gateway

You might also need to add the IP addresses of one or more DNS servers.

- 16 When a computer on the network accesses the Internet and goes through a server, router, or other device that substitutes its own IP address for that of the computer requesting the information, what's the name of the device?

A DNS server
B DHCP server
C Proxy server
D Gateway

- 17 What's the name of the device that ensures that all communication is received from outside users and computers that are legitimate?

A Firewall
B Proxy server
C Gateway
D NAT

- 18 Name the two major wireless security methods.

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA)

19 What are eight steps you can take to secure your WLAN?

- a Enable WEP.*
- b Change default access point administrative passwords.*
- c Change default SSIDs.*
- d Disable broadcast SSID.*
- e Separate wireless network from the wired network.*
- f Put the wireless network in a DMZ.*
- g Disable DHCP in WLAN.*
- h Enable MAC address filtering.*

Independent practice activity

- 1 Identify the operating system in use on your computer.
- 2 Determine the name of your computer and the name of the workgroup to which your computer belongs.
- 3 Determine the type of network cable and connector by which your computer connects to the network.
- 4 Determine which network protocols are installed on your computer.
- 5 If you don't have Internet connectivity, continue to identify and resolve problems until you can successfully access the Internet.
- 6 Verify that your computer's virus protection is up-to-date.

Unit 3

Audio/video system concepts

Unit time: 180 minutes

Complete this unit, and you'll know how to:

- A** Describe home theater system components and characteristics.
- B** Identify content management systems and how they are used in home theater systems.
- C** Set up and configure multi-room audio and video systems.

Topic A: Residential home theater systems

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
2.1	<p>Implement, maintain, and troubleshoot multi-room audio systems. Identify common interference sources.</p> <ul style="list-style-type: none"> Control devices <ul style="list-style-type: none"> Keypads Rotary volume controls Sliders Touch screen Wireless keypads Handheld devices Differentiate and define single source, multi-source, and local source <ul style="list-style-type: none"> Analog audio system Analog Cat5 audio system Digital Cat5 audio system Proper cable use <ul style="list-style-type: none"> Line level vs. speaker level Amplification <ul style="list-style-type: none"> Ohm's law <ul style="list-style-type: none"> Impedance matched or non-impedance matched Watts vs. dB Local amplification Centralized amplification Speaker types <ul style="list-style-type: none"> In-wall Surface mounted Ceiling mounted Freestanding Fixed Animated Speaker specifications <ul style="list-style-type: none"> Frequency response Efficiency Power handling
2.2	<p>Install, configure, and maintain a residential home theater system.</p> <ul style="list-style-type: none"> Audio components <ul style="list-style-type: none"> Define basics of acoustics <ul style="list-style-type: none"> Sound reflection Sound cancellation Speaker placement Sound balance

- Audio/video components setup and integration
 - Digital signal cables and lengths
 - Legacy devices
- Multi-channel surround
 - SACD
 - DVDA
 - DTS
 - DTSES
 - DDEX
 - DD
 - Crossovers and speaker setup
- Video components
 - Display types
 - Plasma
 - LCD
 - LCoS
 - CRT
 - Rear projection
 - Front projection
 - Direct view
 - High definition resolution options
 - 720p
 - 1080i
 - 1080p
 - Tuner types
 - NTSC
 - PAL
 - ATSC
 - QAM
 - CableCard
 - VSB
 - DVB-T
 - DVB-S
 - Video processing
 - Scalers
 - Processors
 - Up-conversion
 - Aspect ratios
 - Video setup - Calibration
 - Color balance
 - Contrast
 - Brightness
 - Digital video cable and connector types
 - DVI and HDMI – compatibility and interoperability issues
- MRAV (Multi-Room Audio Video) standards if/when applicable

Acoustics

Explanation



Acoustics refers to the creation, control, recording, reception, and effects of sound. It is affected by both the equipment used and physical area in which the sound is reproduced.

Sound reflection

The sound continues after the source has stopped producing the sound. This results in the reflection of the sound signal from various surfaces in the room. A surface that is concave concentrates the reflected sound waves. A surface that is convex spreads the reflected sound waves. Sound reflection can result in echoes as well. Early reflection results in a degraded image because sound waves reach the ears of the listener out of synch with the direct sounds. Place the speakers so that sounds coming directly from the speaker arrive at the listener's ears first and reflections arrive later and at a lower volume. However, the reflections should reach the listener within about 5 milliseconds or the sound will become muddled.

If the room has a lot of bare surfaces you might get a harsh sound. Carpets and drapes can help alleviate this problem. A room that is square or in which the length is exactly twice the width can exacerbate resonance problems as well.

The size of the room and the objects contained within the room will affect the sound reflection. Furniture tends to absorb sounds and hard surfaces tend to reflect sounds.

Speaker placement

Placing the speakers close to the wall, floor, or ceiling brings out the bass. Changing the location of the speakers can drastically change the quality and amount of bass the listener hears. Also, placing the speaker a bit away from the back and side walls will help prevent early sound reflection.

The relationship of the speaker to the sidewall tends to affect midrange tonalities while the relationship to the back wall tends to affect bass tonalities. For most listeners, the ideal speaker placement is for the speakers to create an equilateral triangle between the speakers and the listener. This will vary between speakers and the manufacturer's suggested starting locations and the preferences of the listeners.

Formulas have been created to help with the initial speaker placement, and they are listed in the following table.

Distance from sidewall to center of speaker	Distance from back wall to center of woofer
$0.276 \times \text{room-width}$	$0.450 \times \text{room-width}$
$0.277 \times \text{room width}$	$0.353 \times \text{room-width}$
$0.276 \times \text{room-width}$	$0.618 \times \text{ceiling-height}$

Second formula is used if first formula places speakers too far into the room

A detailed example of speaker placement procedures can be found at immediasound.com/Speakersetup.html.

You can also create a grid that divides the room into thirds or quarters. Then place the speakers on intersecting lines in the grid for initial speaker placement. If possible, the listener should be placed at the center of the rear wall of the room within one to three feet from the wall. This will allow him or her to experience the best sound with the least sound reflection. Over the course of a few weeks, adjust the speakers about a half-inch at a time until the listener is satisfied with the results.

Toeing in or aligning the speakers with the walls of the room will greatly affect the sound you get from the speakers. Experiment using recordings that the listener is very familiar with so that he or she can hear the differences between various speaker placements.

The International Telecommunications Union (ITU) created a recommendation for multi-channel audio system speaker placement. Recording engineers set up their recording studios to match this standard. Therefore, for listeners to get the sound the way the engineers captured it for playback, your system should be set up in the same configuration. However, most homes were not designed with home theater and loudspeaker placement in mind (although new construction often does take this into consideration). So in most cases you won't be able to replicate the setup exactly. Also furnishings and other objects in the room affect the sound.

The values shown are ITU values. Dolby recommends 22 to 30 degrees for the front and 110 to 120 degrees for the rear.

All of the speakers in the configuration are an equal distance from the center. You can picture this as a circle of speakers with the listener at the center. The center speaker will be directly in front of the listener. The left front speaker is 30 degrees to the left and the right speaker is 30 degrees to the right. Left and right rear speakers are 110 degrees from the center speaker. The front left, front right, and listener should create an equilateral triangle.

Dolby recommends starting with the subwoofer near the listener.

In the ITU model the subwoofer is placed on the arc between the center and left front speakers. Try the subwoofer at various locations to find where the crossover is the smoothest and the subwoofer doesn't stand out audibly.

All of the speakers should be unidirectional speakers. These also might be referred to as front firing or direct radiating loudspeakers. In reality, most homes have full size front speakers and smaller front and rear speakers.

Symmetric placement of speakers in a symmetric room can create sympathetic standing waves. This creates an uneven room response. Asymmetric placement of the subwoofer can help alleviate this problem. A second subwoofer can also be used to even out problems with room response.

The tweeters on the front speakers should all be at the same height between the speakers. If possible, this should be at ear height for the seated listener.

Line level audio

Line-level audio is also known as analog audio. You can run audio signals over RG6 coaxial cables, but this is not usually acceptable due to the unbalanced signal carried. It is susceptible to 60Hz interference common in home environments as well. This audible interference makes this a poor choice in most situations. You can get it with dual or quad shielding to help prevent interference.

Stereo system cabling

To prevent signal loss, proper gauge cable should be used. The proper gauge will depend on the distance between the speakers and the amplifier. It is recommended that you use the following gauge wires.

Gauge	Distance
12	Over 200 feet
14	Between 80 and 200 feet
16	Under 80 feet

You can use thicker gauge than that recommended; never use thinner.

Amplification

Ohm's law describes the relationship among amperes (amps), or the amount of current flowing, volts, which is the electrical potential between the two ends of a circuit, and ohms resistance within the circuit to the flow of current:

Ohm's law: $V = IR$ or Volts = Amperes \times Ohms

Electric power used is usually expressed in watts, which are commonly calculated in a circuit by multiplying the volts by the amps. Using this formula, a light bulb in a 110-volt circuit through which 0.9 amps of current flow can be said to consume about 100 watts of power. This simplified calculation doesn't allow for resistance in the circuit, but it gives results accurate enough to calculate load requirements in a home system.

Impedance is the resistance to an input signal. In a speaker, this would be the resistance of the coil; the more resistance, the more heat that is generated. By matching impedance the resistance is minimized and optimum sound quality is achieved with minimal heat generation. Today's amplifiers and speakers are marked for Ohm's resistance and should be matched accordingly for best sound reproduction.

When stringing together multiple speakers, impedance might drop to such low levels that great amounts of heat are generated, causing the amplifier to overheat.

Non-impedance matched speakers can be used with an impedance matching audio module. This raises the impedance of the circuit. As you add more speakers to the system you lower the impedance. This is particularly true in a multi-room setup. Adding an impedance matching module will correct the low impedance problem in multi-room configurations.

Another method around this problem is using a multi-channel amplifier. This has enough channels to connect speakers for each of the locations in which you wish to place speakers without causing an impedance problem.

A *decibel* (dB) is a logarithmic scale used to express the relative strength of an acoustic wave. An increase of 1 dB doubles the volume produced by the speakers. Watts are the unit of power used to rate the output of an amplifier. Watts are also used to rate speaker power. You should try to match the wattage of the amplifier and the speakers.

Both decibels and watts are measures of the power of the speakers. Decibels are a real measure of sound pressure. Watts measure the electrical handling capability of the speakers. The actual loudness of the speakers would be determined by the efficiency of the speaker.

When you are evaluating speaker wattage, another specification you might encounter is watts RMS. The Root Mean Square (RMS) determines the speakers' average power output over a period of time. Another number you might encounter is peak momentary power output (PMPO) which is peak output measured in microseconds.

You can set your home sound system up with local amplifiers for each set of speakers. This can be expensive if you put a high quality amplifier in each location. Another alternative is to have a centralized amplifier for all of the sets of speakers in all of the rooms. Most experts recommend having up to 3 sets of speakers on a single amplifier. For more than that, you should consider setting up another amplifier.

Crossover

Crossovers send frequency ranges to the appropriate speakers. This frequency division is called the crossover. Many crossovers use filters to shape the frequency response. The filters also help stabilize the speaker's load impedance. Level controls are used in some crossovers to attenuate parts within the signal.

Active crossover is a frequency divider at line level. It uses integrated circuits, transistors, or tubes. Impedance is buffered and provides consistent transition no matter what the load.

Sound cancellation

In some cases, you want to cancel out sounds. For example, noise canceling headphones block out the ambient room sounds so they don't intrude on what you are listening to through the headphones. They sample ambient noise and create sounds 180 degrees out of phase with it. In other cases you may not want sounds canceling each other out. This can happen accidentally if your speakers are out of phase.

On speakers that are in phase, the driver of the left speaker moves in at the same time as the driver of the right speaker. If they are out of phase then the driver of the left speaker moves in at the same time as the driver of the right speaker moves out. This is usually caused by a reversal of the polarity on one speaker's input terminals. An out-of-phase system will result in vague imaging with loss of bass due to the sound cancellation.

Sound balance

Sound balance is a term used to describe the comparison of sound levels between audio channels. It can also be used to describe the mix between frequencies (high, midrange, low) to create an even sound envelope where all frequencies are at proper levels for the room.

The difference in volume between sounds from left and right help the listener place themselves in relation to the sound and to create a three-dimensional auditory perspective. If one of the channels is too loud, it affects how you hear the playback of the sound.

Do it!

A-1: Defining acoustical terms**Questions and answers**

- 1 Why are acoustics important when setting up a sound system?

To get the optimum sound from the system

- 2 When wiring the sound system what must you be aware of?

Make sure the polarity is correct when hooking up the speakers to avoid out-of-phase sound.

- 3 What three things do you need to consider for optimal sound?

Room acoustics, speaker placement, and sound balance

Multi-channel surround

Explanation



Multi-channel surround sound usually consist of five speakers. A right and left front, right and left rear, and a central speaker coupled with the surround sound decoder/amp will give the listener the sensation of three-dimensional sound.

Crossovers in multi-channel surround systems

A crossover is basically an electronic gate that can send high frequencies to the tweeters, midrange frequency to the midrange speakers and low frequencies to the woofers or subwoofers. Crossover of signals from speaker to subwoofer may or may not be adjustable. The crossover is based on frequency at which the crossover should occur. This is usually a range from 80 Hz to 120 Hz. The recommended crossover frequency is 120 Hz. It can also be configured to be bypassed with the bass management filter handling roll-off. Having bass-managed channels near 80Hz enables you to have more options in placing the subwoofer without it becoming audibly apparent.

Speaker setup

Setting up speakers is fairly easy. First place the speakers in their approximate positions. The subwoofer is non-directional, so it may be placed in the front or rear of the listening area. The midrange speakers and tweeters are usually placed on the left and right.

Attaching the input wires to the terminals is next. Keep correct polarity in mind to avoid an out-of-phase problem. You can use standard speaker wire in a variety of gauges. Thicker wires put less strain on your amplifier. Optical cables can also be used. The connectors vary based on what options your receiver and speaker use. Some use RCA-type connectors. Others just require that you expose the wires from the protective covering and then insert the bare copper wires into a clamp or under a screw-down device. Others use banana-plugs. Examples of speaker connections can be seen in Exhibit 3-1.

- The one on the left is an RCA connector. It is the connector on an optical cable that connects to a subwoofer. It plugs into the RCA port on the speaker.
- The center example is bare wire in which the covering has been removed to expose the bare copper wire. It connects to the speaker by pressing down the red or black lever to expose a hole through which the cable can be inserted.

- The right example uses banana plugs. These screw onto the end of the cable speaker wire to grab onto the wire. In this example, there is a hole in the binding post and the plug is secured into place by screwing down the connector to hold the plug in place.



Exhibit 3-1: RCA, bare wire, and banana plugs.

Surround sound

The most common configuration sources are recorded in is 5.1. The 5.1 format is used in everything from game consoles to HDTVs to movie theaters. In this configuration, there are five main channels and one low frequency effects (LFE) channel. The subwoofer is responsible for playing back the LFE channel. This is usually set up with five speakers and a subwoofer. The 6.1 format adds a rear speaker channel. The 7.1 format sends the sixth channel to two rear speakers.

Matrixed channels

Matrixed channels is the term for output channels that are derived electronically from input channels. Two inputs are electronically processed to create output to four channels. Each of the four channels is different yet together they retain all of the two-channel information.

DTS

Digital Theater System (DTS) is a surround sound format that uses up to five channels of full frequency sound along with a sixth channel for low frequency effects (LFE). This is a 5.1 channel format. The “5” designates the front center, left, and right, and surround left and right. The “.1” designates a channel that contains only deep bass frequencies and not a full range of frequencies.

DTS digital sound requires a receiver or preamp that has DTS decoding built into it, a DVD player that uses DTS digital output as well as optical or coaxial connections between the receiver or reamp and the DVD player. An alternative is to use a 5.1 channel receiver or preamp with a DTS DVD player and three pairs of RCA analog connections, but this isn’t the preferred configuration.

DTS-ES

DTS-ES is the Extended Surround format or 6.1 channel configuration. ES adds one or two additional speakers to the rear of the listener. These are referred to as back surround channel speakers.

There are two types of DTS-ES:

- DTS-ES Matrix, in which the back surround channel is matrixed to the left and right surround channels. It can use THX Surround EX components and is compatible with DTS 5.1 components.
- DTS-ES Discrete 6.1, in which the back surround channel is a discrete signal. DTS 5.1 components ignore the back surround channel.

You will probably see some equipment listed as 7.1 surround. This is not a true surround sound format. It uses the ES back surround signal either for both additional speakers or some left and right surround signals may be mixed in. This is a proprietary implementation of signals and not an industry standard.

Dolby Digital

Dolby Digital (DD) is another 5.1 surround sound format and is the DVD-Video standard format. DD refers to having the encoding for up to 5.1 channels. If the packaging explicitly states Dolby Digital 5.1, then you can be assured that the soundtrack contains 5.1 discrete channels.

DD-EX, also known as THX Surround EX, is the Dolby implementation of the 6.1 surround sound format. It requires a DVD player with a digital output such as optical or coaxial. It also requires a receiver or preamp with a THX Surround EX decoder.

This uses the matrix method of sending signals to back surround channels. Therefore, it is not truly a discrete 6.1 format.

Super Audio CD

Super Audio CD (SACD) is a high quality optical audio disc designed by Sony and Phillips. There are three types of SACD:

- The hybrid version includes a CD layer, which is compatible with standard CD players. It also includes an HD layer, which is a 4.7 GB SACD layer.
- Single layer contains only the 4.7 GB SACD layer and no CD layer.
- Dual layer contains two HD layers for a total of 8.5 GB and no CD layer.

SACD discs contain a two channel stereo mix. It might also contain a surround mix in surround sound in either 5.0 or 5.1 format. SACDs usually have a Multi Channel logo on the back cover to designate it as a multi-channel recording.

DVD-A

DVD-Audio (DVD-A) is a competitor to SACD. Sometimes DVD-A is referred to as DVD-Music, but that is not an official DVD format. Instead, it is how people are referring to DVD-Video discs containing music. It plays on any DVD player and often contains video of the performers.

DVD-A discs contain special audio tracks in a high fidelity format that can be played only on DVD-Audio players. Most DVD-A discs are designed so that they can be played in any DVD player. They then contain a separate AUDIO_TS directory that contains a DVD-Audio zone that regular DVD players don't read.

A player that plays both DVD-Audio and DVD-Video discs is called a Universal Player or Video-capable audio player (VCAP).

Speaker types

There is a wide array of options when it comes to choosing the speakers you add to your sound system. There are the standard free-standing speakers that have been around for years. There are also smaller bookshelf sized speakers that are nearly as powerful as the big floor models.

In many homes, it is undesirable to have large speakers taking up valuable floor space. Also, they might not match the aesthetics of the room. In these cases, you might opt for speakers that are placed in the wall or in the ceiling.

If floor space is at a premium, some of the speakers can be mounted to the wall. These are surface mounted as compared to those that are in-wall speakers. The in-wall speakers use the structure of the wall in place of the usual speaker cabinet. This can greatly affect the sound of the speaker as the cabinet is an integral part of producing the sound. This is also true of the ceiling mounted speaker.

If you have a party atmosphere in your home, you might choose to have some sort of animated speakers in the family room or bar area. Animated speakers usually either have lights or some sort of animatronic movement that is activated by changes in the frequency of the music being played.

Speakers optimized for surround sound music and those optimized for movies differ. For movies, the best results are obtained from dipolar speakers. Sounds are produced equally front and rear from side speakers. Sound is reflected from the room boundaries, emulating the many speakers in a theater with just the surround speakers.

Treble balance can be adjusted by changing the height and angle of speakers. Bass balance can be adjusted by changing speaker location relative to side and back walls. The depth of the soundstage can be adjusted by moving speakers out into the room.



Single, multiple, and local sources

In a whole-house audio system, there are three choices for the source. They are single, multiple, and local sources.

- Single source is one amplifier controlling volume and content for all rooms. Volume controls in each room enable you to set the volume.
- Multiple source requires a separate amplifier for each room or zone. This enables you to control not only the volume, but also the content so that each room can play different music.
- Local source is the simplest and the least useful in a whole-house system. This requires you to go to the amplifier, where you can change the content and the volume. There is no control of either at remote locations within the home.

Analog audio system

For an analog audio system, you connect the components to the amplifier by using analog RCA cables. When you want to share this information with other locations in the home, connecting components in other rooms requires an alternate method since the maximum length of these cables is about 6 feet before the signal begins suffering signal loss.

Analog CAT5 audio system

To reach all of the locations you want to send your A/V signals, you might need something other than standard cabling. CAT5 cabling enables you to transmit signals up to 1,000 feet away.

A *balun* is used at each end of the run. A balun is a transformer that enables you to send a signal of one impedance over a cable that requires different impedance. They are used in pairs: one at the source and one at the destination to change the impedance back to the original value.

Digital CAT5 audio system

Digital signal baluns are also available. This is needed for HDTV and digital audio signals. While the signal can reach 1,000 feet, the quality degrades on long cable runs. The following table shows the signal quality at varying distances.

Distance	Signal
500 feet	720p video, 720p video with digital audio, 1080i/p video, 1080i/p with digital audio
600 feet	Digital audio only, 480i/p video with digital audio
1,000 feet	480i/p video only

Speaker specifications

When you are looking at speaker specifications, there are several key specifications that you need to understand and compare. These include:

- Frequency response
- Efficiency
- Power handling

Frequency response is usually rated against the average frequencies humans are able to hear. This is approximately 20 Hz to 20 kHz. The original CD specification covered only that frequency range. Updated formats such as SACD and DVD-Audio are capable of accommodating a wider frequency range. The sign of a good speaker is the evenness of the sound reproduction over the full frequency range. Some speakers are designed to reproduce only a portion of the frequency spectrum. Examples of this are subwoofers, mid-range, and tweeters. Each is designed to reproduce a specific range of frequencies optimally.

The efficiency of a speaker determines how well it turns the line signal into sound. This is rated as RMS. You might also find it in dB. Highly efficient speakers require less power to reproduce sounds at the same volume than a speaker with lower efficiency would require. It might be noted that highly efficient speakers can sacrifice a flat frequency response for efficiency.

Power handling is specified in several ways. The measurements include PMPO, RMS, and minimum recommended power. RMS is usually about one-half of the peak power. The power needed to efficiently drive the speakers is the minimum recommended.

Proper cable use

You can have the best equipment in the world, but if you don't use the proper cables and connectors, you will not achieve the sound qualities the equipment is capable of achieving.

With cables, when you are comparing gauges of cable, the smaller the number, the thicker the wire. You can always use a thicker gauge wire for connecting speakers, but you should never use a thinner gauge than what is recommended.

Line level

Line level is low level signals that occur before the signal reaches the amplifier. Also, the signals between components before amplification are line-level signals. These signals do not respond to the stereo system volume control. A phonograph cartridge requires a preamp just to get the signal up to line level.

Audio equipment uses low currents. To get the best frequency response and minimum distortion, devices send low output impedance as input to a receiver with high input impedance.

A typical home quality audio device uses -316V or -10dBV . Professional quality devices typically operate at 1.23V or $+4\text{dBu}$. dBu is an impedance that is unspecified and un-terminated. dBV refers to that value times 1 volt.

Speaker level

The power of the amplifier's output determines the *speaker level* signal's voltage. To calculate the voltage, take the square root of power and multiply it by resistance. So, for example, a 100-watt signal going to 8-ohm speakers would result in a 28.3V signal.

Do it!

A-2: Identifying multi-channel surround options

Questions and answers

- 1 What does the “.1” portion in the number of channels in a multi-channel surround sound system refer to?

The .1 refers to the subwoofer.

- 2 When a speaker system is described as being matrixed, what does this mean?

Matrix is the term for output channels that are derived electronically from input channels. Two inputs are electronically processed to create output to four channels. Each of the four channels is different yet together they retain all of the two-channel information.

- 3 What is the purpose of crossover between speakers?

A crossover is basically an electronic gate that can send high frequencies to the tweeters, midrange frequency to the midrange speakers, and low frequencies to the woofers or subwoofers.

- 4 List some things you need to consider when installing in-ceiling or in-wall speakers.

You need to consider the location since it is not easy to move them after installation. Also, the wall or ceiling space takes the place of the cabinet speaker in a freestanding speaker.

- 5 Compare line level and speaker level.

Line level is the low-level signals that occur before the signal reaches the amplifier. Speaker level signals are those whose volume can be changed by the amplifier.

Display types

Explanation

There are eight different types of video displays that are currently available. Each has its pros and cons. Some are direct view and others use projection

Direct view and projection televisions

Direct view televisions are any set that doesn't use projection technology to display the image. CRT, plasma, and LCD TVs all fall into this category.

Projection televisions are either front projection or rear projection sets. There are rear projection CRTs and microdisplays including rear projection LCD. A microdisplay system produces a tiny image using LCD technology and then projects it through a projector to the larger viewing size. DLP and LCoS technologies are typically front projection systems.

CRT

The traditional display, the *cathode ray tube (CRT)* is still a good all around choice for price and performance. The vast majority of CRT televisions will be standard definition sets with 480 lines of resolution. CRT displays use one of two methods to display: interlaced or progressive scan methods.

The aspect ratio, the shape of the screen, is 4:3 for standard definition televisions. This is the National Television System Committee (NTSC) standard.

CRTs display images on the flat front face of a glass cathode tube. This display is created by a beam of electrons shooting from the back of the cathode tube toward its front screen face. Plates on the top, bottom, and sides of the tube control the direction of the beam and direct it to continuously "paint" lines from left to right, top to bottom, across the screen. A grid placed in front of the filaments that generate the electron beam controls the intensity and color of the beam as it paints an electron stream across each line on the screen. Phosphor dots on the inside face of the screen light up when struck by the beam and produce dots of color on the display face. These dots of color are visible on the outside of the tube. The beam's color is controlled by the grid and can cause any combination of red, green, and blue phosphors on the screen to light at the appropriate level to produce the desired color for that area of the screen image. Exhibit 3-2 shows how a CRT monitor works.

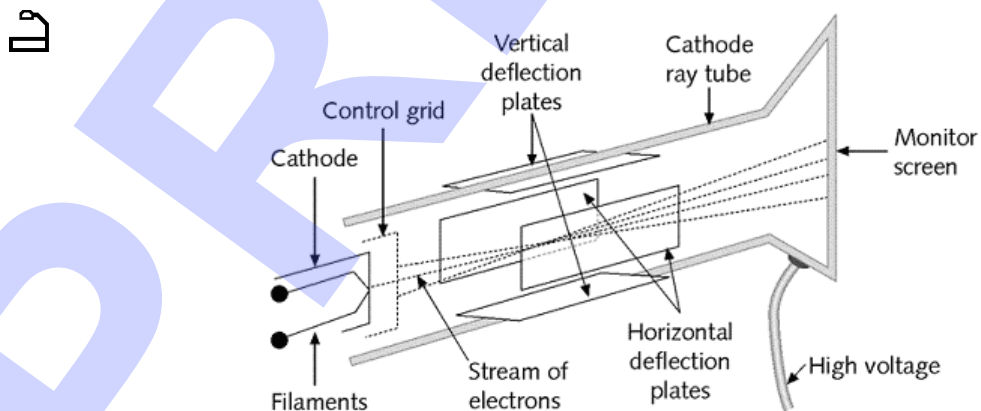


Exhibit 3-2: The operation of a cathode ray tube (CRT)

The refresh rate of a PC monitor can be adjusted from the control panel in Windows.

CRT displays come in many sizes, from 8-inch screens (screen size is always measured diagonally from one upper corner to the opposite lower corner) up to 42 inches. Screen size measures the actual surface of the screen. The image displayed on the screen is usually about two inches smaller than the measured size of the screen.

The refresh rate or scan rate is the number of times per second that the electron beam in the tube repaints the entire screen. The higher the refresh rate, the less flicker is apparent in the screen display and the more steady it appears to the viewer. Most CRT PC monitors being sold today are set to refresh at a rate of 60 Hz, which means the screen is completely repainted 60 times each second. This is adequate to prevent almost all flicker unless the display on the screen has an extreme amount of very rapid movement. In that case, the refresh rate can be set higher to eliminate the problem.

Flicker in a monitor is also affected by whether the refresh method is interlaced or non-interlaced (progressive). Interlaced monitors paint their screens in two passes; they draw the odd-numbered lines on the first pass and the even-numbered lines on the second. This has the effect of changing only half the screen at a time and tends to minimize any flicker when the refresh rate is slow. Non-interlaced monitors paint their screens completely in one pass. When the refresh rate is high (60 Hz or more) they appear steadier and have less flicker than an interlaced display. Non-interlaced (progressive) monitors also appear to cause less eyestrain when viewed for long periods, though why this occurs is unclear. Computer monitors are non-interlaced.

Television monitors are nearly always interlaced and nearly always have a refresh rate of 30 Hz. This slow refresh rate plus their limited resolution make CRT television monitors unsuitable for use as computer displays and very few are used as such today.

High-definition TV monitors have the same dot pitch, refresh rate, and interlaced method of refreshing as standard monitors. Their higher resolution and improved picture quality come from increasing the number of lines painted on the screen and changing the aspect ratio of the display from the 4:3 ratio (width to height) found in standard television and computer monitors to a 16:9 width-to-height ratio.

The following table defines some of the characteristics of CRTs.

Characteristic	Description
Screen size	Diagonal (top left to bottom right) width of screen surface
Refresh rate	The number of times per second an electron beam fills a video screen with lines from top to bottom
Scan rate	The number of times per second an electron beams moves from top to bottom of a video screen; equal to refresh rate in progressive screens, and to 1/2 refresh rate in interlaced screens.
Interlaced	Screens in which the electron beam draws every other line with each top-to-bottom pass to reduce flicker from slow refresh rate.
Progressive	Screens in which the electron beam draws every line with each top-to-bottom pass.
Dot pitch	The distance between adjacent same-color dots on the screen.
Resolution	The number of pixels (picture elements) that can be addressed on a screen by software.
Multi-scan	A CRT that supports a variety of refresh rates and resolutions so that it can function with a variety of input devices.

Plasma

Plasma displays are thin and have a great contrast ratio and good viewing angle. They have problems with screen burn-in so they are not the best choice for gaming or for use in any application in which there would be a static image displayed on the screen for long periods of time. They are best viewed in a darker room.

These typically use the high definition standards and have an aspect ratio of 16:9. They usually have 720 lines of resolution and use the progressive scan method.

Plasma screens are composed of electrical circuits inserted between two sheets of glass. The electrical charge creates the plasma, which gives off light. These are quite heavy pieces of equipment that might require extra support structures if you want to mount them on the wall. They are thin, usually about 4 or 5 inches thick, so much thinner than a standard CRT set which is needs to be quite deep to focus the cathode ray guns on the phosphors coating the screen.

LCD

Liquid crystal display (LCD), while still more expensive than CRT monitors, are becoming more common and less costly. They are now available in sizes comparable to CRT monitors, and they have the advantages of being much lighter, more compact in size, and consuming less electricity than CRTs. LCD displays form images by activating pixel-sized areas in a layer of liquid material sandwiched between two arrays of electrodes, one arranged in columns behind the liquid layer, and the other arranged in rows in front of it. By activating the electrodes on either side of the liquid layer, the controller allows a particular color of light to pass through the layer at each pixel location. The lighted pixels produce an image on the panel. Exhibit 3-3 illustrates how an LCD display works.

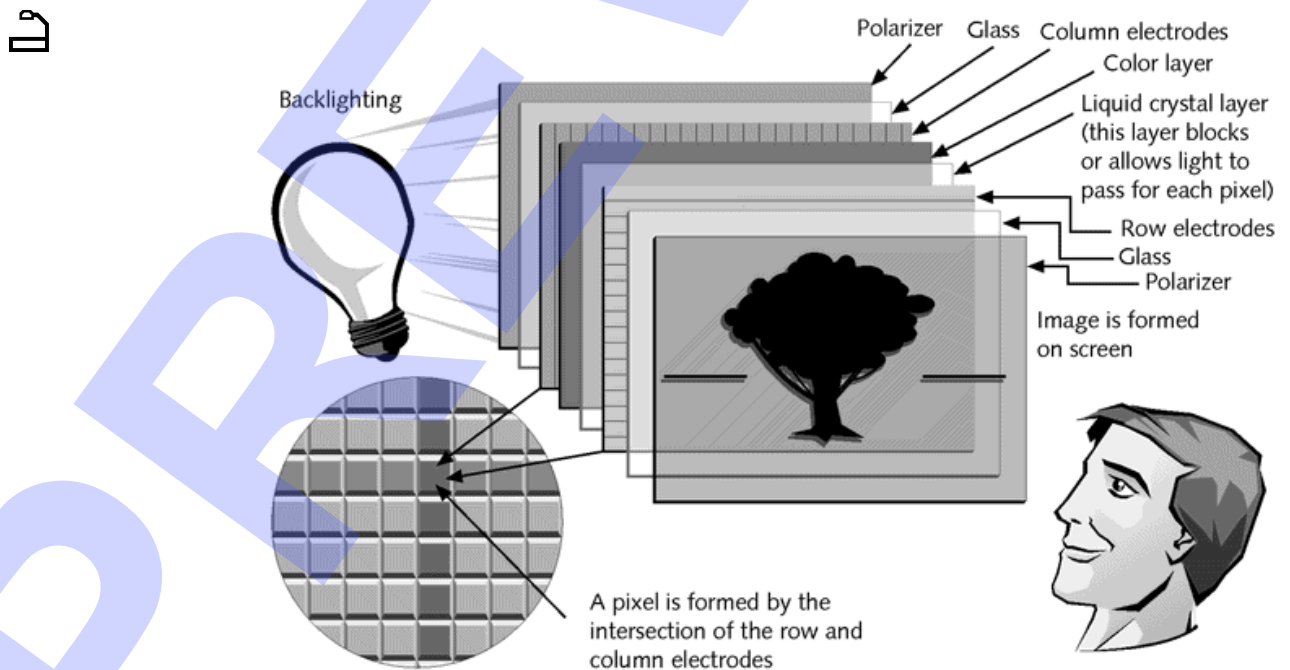


Exhibit 3-3: How an LCD flat panel screen works

Early LCD panels were dim compared to CRT displays. Dual-scan, passive matrix displays improved performance by adding a second set of vertical electrodes to the sandwich, but these monitors still were not as bright as CRTs. LCD panels now are active matrix displays in which a transistor is added to enhance the brightness and color of each pixel. Active matrix displays can be used in lighted rooms and compare favorably with CRT monitors for brightness and resolution.

LCD panels can display only digital data. They can be used for analog (television) displays only if the data signal is first converted to digital form. High-definition LCD panel television screens up to 60 inches in size (16:9 aspect ratio) are becoming more common in home theaters.

DLP

A *digital light processor (DLP)* display is a front projector projection system. This projector uses an array of microscopic mirrors, one for each pixel, and a special video chip to determine whether the projector's lamp should illuminate a particular mirror or not. The resulting mirrors reflect the light to create the image which is projected from a projector onto the screen. The size of screen that can be accommodated in a room is determined using something called the *throw ratio*. This is the relationship between projector and the screen and the width or the projected image.

The light bulb in a DLP projector needs to be replaced periodically. The bulb typically lasts about 3,000 hours.

The image can be displayed on a pull-down screen or directly on a blank white wall. You will get a better looking image on a screen though.

LCoS

Liquid Crystal on Silicon (LCoS) displays are another projection type system. These are basically LCD/DLP hybrid system that has been reduced to a chip. It is like LCD in that it uses liquid crystals. The crystals are affixed to a mirror surface like in DLP.

Separate LCoS chips are used for red, green and blue channels. Compare this to DLP, which uses a spinning red/green/blue disk to create the colors, so each color is sent separately in DLP. LCoS systems are able to send all three colors simultaneously. The bulb in a LCoS projector typically lasts up to 1,500 hours.

They are used for reflective rather than transmissive video projection systems, giving a very high quality image suitable for HDTV. They are available in 720p and 1080p resolution. However, the contrast ratio is much lower than other HDTV technologies. LCoS images tend to look more natural than images on DLP systems in which sharp lines are created by the edges on the individual DLP mirrors.

Do it!

A-3: Identifying display types

Questions and answers

1 Which of the display types is considered a flat panel?

Plasma and LCD

2 Which of the display types are projection systems?

DLP and LCoS

3 Which of the display types are direct view systems?

CRT, plasma, and LCD

4 About how long do light bulbs last in DLP and LCoS projectors?

DLP bulbs usually last about 3,000 hours and LCoS bulbs usually last up to 1,500 hours.

Video tuner types

Explanation

Incoming video stability can come in over standard video or high definition video technologies. Standard video uses the NTSC standard. High definition video uses the ATSC standard.

NTSC

The most common analog television format in the United States is the *National Television Standards Committee (NTSC)* standard, which has 525 horizontal scan lines in its picture and runs at the speed of about 30 frames per second. This standard has been in place for more than 50 years and is now badly outdated.

Most analog television broadcast stations transmit a picture that contains 480 horizontal interlaced lines with approximately 340 pixels per line. Europe and some other parts of the world have adopted the PAL or SECAM formats for television, which both have a practical resolution of about 720 pixels (picture elements) wide by 576 high (625 scan lines high counting overscan). These formats operate at 25 frames per second to more easily function on the European standard power grid, which is 50 cycle AC current at 240 volts. Even though the PAL/SECAM formats have higher resolution than NTSC, they're not updated (refreshed) as often and so their picture quality is comparable.

ATSC

When the United States decided to make the transition from analog television to *digital television (DTV)*, the Federal Communications Commission agreed to let broadcasters decide whether to broadcast *standard definition television (SDTV)* or *high definition television (HDTV)* programs. Most have decided to broadcast SDTV programs in the daytime and to broadcast HDTV programs during prime time in the evening. Both SDTV and HDTV are supported by the Digital Video Broadcasting (DVB) and *Advanced Television Systems Committee (ATSC)* set of standards.

SDTV is a digital television (DTV) format that provides a picture quality similar to that recorded on digital video disc (DVD). SDTV and HDTV are the two categories of display formats for DTV transmissions, which are becoming the standard in the United States. SDTV has a range of resolutions and no precisely defined aspect ratio, although most stations broadcasting SDTV send a signal with approximately the same number of scan lines (vertical pixels) as NTSC and about 720 horizontal pixels. New digital-receiving television sets will be either HDTV-capable or SDTV-capable, with receivers that can convert the received signal to their native display format. SDTV and HDTV both use the MPEG-2 file compression method.

HDTV provides a higher-quality display than SDTV, with a vertical resolution display from 720 lines progressive to 1080 lines interlaced or higher and 1920 horizontal pixels per line, making the resolution much better. The HDTV aspect ratio (width to height ratio of the screen) is 16:9, which is about the same as a movie theater screen. HDTV, in common with SDTV, uses the MPEG-2 file compression method.

The following table shows a comparison of several television formats with popular computer screen resolutions, photo print sizes, and digital camera formats. It also shows the number of pixels required to create one frame of data in each of these formats.

Format and other info	Aspect ratio (H:V)	Horizontal pixels	Vertical pixels	Total pixels
3x5 photo scanned at 100 dpi	5:3	500	300	150,000
SVGA computer screen	4:3	640	480	307,200
Standard MPEG-2	16:9	724	408	295,392
NTSC television standard	4:3	720	525	378,000
SDTV	4:3	720	525	378,000
Anamorphic DVD	16:9	960	540	518,400
8x10 photo scanned at 100 dpi	5:4	1000	800	800,000
XGA computer screen	4:3	1,024	768	786,432
1.3 megapixel digital camera	4:3	1,280	960	1,228,800
HDTV	16:9	1,920	1,080	2,073,600
2.35:1 HDTV	2.35:1	2,538	1,080	2,741,040
3.3 megapixel digital camera	4:3	2,048	1,536	3,145,728

HDTV resolutions come in several common options. Some of them are progressive scan, in which all of the lines are refreshed every time the image is refreshed. Others are interlaced, in which only every other line is refreshed when the image is refreshed. All of these come in 16:9 aspect ratio.

The 720p designation indicates that there are 720 lines of pixels on the screen that are refreshed using the progressive scan method. There are 1,280 pixels across the screen. HDTV broadcasts, HD DVD, and Blu-ray discs are all compatible with this format.

The other resolution is 1080. It comes in both interlaced and progressive scan versions: 1080i and 1080p. There are 1,080 lines of pixels on the screen in this format. These sets have 1,920 pixels across the screen.

QAM

Quadrature Amplitude Modulation (QAM) is the format by which digital cable is encoded and transmitted via cable. This is the equivalent of an ATSC tuner for receiving digital transmissions. QAM enables you to receive unscrambled digital programming.

CableCard

Using a *CableCard* enables you to receive digital programming from the cable provider. The card enables you to descramble the encrypted signals from the cable provider. This can replace the set-top boxes usually required to receive the signals and unscramble them for viewing. CableCards come in the PC Card (PCMCIA) and PCI standards for use in computers. Some digital cable ready TVs also have a slot for the PC Card version of the CableCard. In addition, some set top boxes have a CableCard slot.

VSB

VSB (vestigial side band) is the RF modulation format used by digital TV to transmit digital bits to the home consumer. The eight-level VSB is the basis for all digital TV broadcasts. It has eight amplitude levels that support up to 19.28 Mbps of data in a 6 MHz channel. A 16-VSB mode has 16 amplitude levels and supports 38.57 Mbps in a 6MHz channel. It is paired with MPEG-II encoding format for broadcast delivery.

DVB

DVB, Digital Video Broadcasting, standards define a suite of open standards for digital video broadcasting. The signals can be broadcast over satellite, microwave, or terrestrial distribution methods. The standard also provides for two-way communication. There are three types of return channels:

- DVB-C for cable communications
- DVB-T for terrestrial communications
- DVB-S for satellite communications

Video processing

The *video processor* is responsible for scaling images for display on your television. Scaling refers to reformatting the image to use more or less scan lines than the original image required, without cropping the image. In digital video, this refers to the number of pixels used on each scan line.

The scaler is responsible for converting from film to digital video. It also reformats DVDs into either 4:3 or 16:9 aspect ratio as appropriate to the television set on which it is being displayed. It is also used to create picture-in-picture (PiP) windows.

The processor is built into DVD players and into many high definition TV sets. You can also purchase external video processors

The video processor also acts as up-converter to change resolutions. This helps bring a low resolution image up to a higher resolution.

Digital video cable

There are a couple of different digital video cables used to connect video displays to PCs and other components. One is the DVI connector and the other is the HDMI connector.

Digital Video Interface (DVI) connectors are 18-pin single cable connectors with D-shaped ends. A DVI connection transmits digital video in completely uncompressed format, which no consumer device can record so it also effectively prevents all copying. DVI connections also include a copy protection scheme called High-bandwidth Digital Content Protection, which prevents transmission to any unlicensed device (one without the copy protection).

If you are connecting via DVI connectors, DVI-D cables are required for HDTVs. DVI-I cables won't work. DVI-D cables cannot carry audio signals; they are designed to carry only the video signal.

High-Definition Multimedia Interface (HDMI) connectors are found on high definition TVs and other high definition components. PCs are now beginning to include HDMI interfaces as well. Digital audio and video can both be transmitted over HDMI cables.

Terminators and connectors

Most connections between audio devices are made with RCA connector cables, usually color coded to help identify the correct connection. Some audio connections are made with BNC connectors, standard and mini phone plugs, and even bare wires (the last usually only for speaker connections). Exhibit 3-4 shows the back of a stereo audio amplifier with a number of input jacks available and a number of outputs.



Exhibit 3-4: Audio amplifier showing input and output connections

Output devices such as CD players and phonograph turntables have output jacks only because they don't receive input. They create signals and output them to other devices. On the left side of Exhibit 3-4 are the audio input connections (left stereo side is white at the top, right stereo side is red at the bottom) for these devices. This amplifier has connections for a phonograph, a CD player, a radio tuner, a DVD player, and an auxiliary input. To connect any of these devices to the amplifier, a pair of RCA connector wires is run from the output jacks on the device to the appropriate input jacks on the amplifier.

In the center part of Exhibit 3-4 are input and output jacks for devices that can have both input and output. These are devices such as tape recorders, which can both play a tape and record one. This amplifier has side-by-side stereo input (left) and output (right) jacks for a tape recorder, a VCR, and a second tape recorder, VCR, or other device. To connect a tape recorder to this amplifier, four RCA connector wires are required. Two of these must run from the left and right output jacks of the tape recorder to the corresponding left (top) and right (bottom) input jacks of the amplifier. The other two must connect the output jacks on the amplifier with the input jacks on the tape recorder.

Any other input and output device requires the same connectors: two from the output of the device to the input of the amplifier and two from the output of the amplifier to the input of the device. Notice how audio connectors always connect output to input. Input never connects to input and output never connects to output. The audio signal is always traveling from one device (output) to the other device (input).

On the right side of Exhibit 3-4 are four sets of speaker connections. These are output connections that allow the amplifier to power two pairs (left and right) of speakers. This amplifier uses bare wire connections for speakers. They are connected by attaching wires to red and black terminals on the amplifier and then attaching them to corresponding connector terminals on each speaker. It doesn't matter which way the speaker wires are connected because the current passing through them to drive the speaker is an alternating current. All speakers must be connected with the same polarity, however, so that their output will be in phase. There must be two wires connecting each speaker, so four speakers require a total of eight wires leading from the amplifier.

An F connector is usually used with RG-59 coaxial cables. These RF connectors have 75 ohm impedance. The connector uses the coaxial cable center as the pin in a male connector. When screwing or crimping it onto the cable you need to carefully fold back the wire shielding, making certain not to allow the foil shield to cause a short with the center connector.

Do it!

A-4: Defining video terms

Questions and answers

- 1 NTSC standard specifies _____ horizontal scan lines at a speed of _____ frames per second
525 lines at 30 frames/second
- 2 Analog television broadcast stations usually transmit at _____ horizontal interlaced lines with a resolution of _____ pixels per line.
480 lines at 340 pixels
- 3 PAL and SECAM resolution is about _____ pixels by _____ pixels at _____ frames per second.
720 x 576 at 25 frames/second
- 4 Which has a higher picture quality, SDTV or HDTV?
HDTV
- 5 What is the aspect ratio for SDTV and HDTV?
4:3 for SDTV and 16:9 for HDTV
- 6 What types of signals are carried on HDMI cables?
HDTV televisions use these cables to connect to other digital devices and the cable can carry both video and audio signals.

Explanation**MRAV standards**

The CEA organization defined a set of standards for adding distributed audio and video in the home environment. The standard makes use of the CAT5 and RG-6 cables commonly installed in homes.

The *Multi-Room Audio Video (MRAV)* standard defines the cables and connectors to be used in distributed multi-room audio and video distribution networks. It provides suggestions on how to network audio sources such as radio and satellite receivers, CD and DVD players, and Internet streaming devices.

The standard specifies how the distribution network is configured. This includes defining zones with at least one speaker per zone whose volume is controlled by a local device.

This is used in new construction and in major home renovations. Applying these standards to existing structures would be too burdensome. Not only would it be expensive to retrofit a home, but you also might need to knock large holes in the walls, ceilings, and floors as you installed in-wall and in-ceiling speakers, pulled cabling throughout the home, and installed control devices in various rooms.

Planning home theater installation

You need to consider all of the things we have discussed in this topic when you are planning your home theater installation. Not only do you need to pick out the equipment, you need to consider the room size, whether you are going to distribute the output throughout the home, and if so how you are going to do so. You also need to consider the types of cabling and control devices that you will use.

All audio components should be carefully grounded to reduce the risk of interference. This is especially important if shielded connector cables are used as connectors because the shielding grounds to the frame of the component. If the frame isn't grounded, the shielding can't perform its function correctly. Instead of grounding interference, it simply transfers it into the component frame where it may be picked up by other parts and still do harm to the system. A bare wire connected from this clamp to ground can ground the device.

Control devices

Most audio/video equipment uses IR signals from a remote control device to control the functions of the equipment. When you implement a whole house A/V system, you need a way to get those IR signals to the source device from another room. Remember, IR is a line of sight technology. To get the signal from the remote room, you will need some sort of device to capture the IR control signals. This might be a wall mounted or wireless handheld keypad or touch-screen device. It could be a simple rotary knob or slider volume controls if you are just running speaker wire and not full control of the media hub devices. It might also include push button controls to select the source device from the remote room.

At the media hub where all of the source equipment is located, you will need an IR connecting block. The cables (Cat5e, RG-59 coaxial, or IR-3 conductor cabling) connect from the remote room control devices to this IR connecting block. This enables IR signals to be sent from any remote room to a single device in the media hub.

One more piece is needed to connect from the IR connecting block to the physical component. This is an IR emitter that converts electrical control signals sent from remote rooms over the cabling back into IR signals that the device can use.

Do it!

A-5: Planning installation and configuration of a home theater system

Questions and answers

- 1 Using the space below, draw a rectangle to represent the room in which your home theater system is to be installed. Indicate where the HDTV, surround sound receiver, DVD player, and each of the speakers in the 5.1 surround sound system would be located. Also indicate where the user will sit in relation to all of these components.

- 2 Identify some of the considerations you would need to think about if the room was square, with bare floors, a single leather couch, and vinyl blinds on a single window.

You would need to account for sound reflection and sound balance. If the sound was too harsh, you might consider adding a rug or drapes to absorb some of the sound.

Topic B: Content management systems

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
2.3	<p>Assess, install, and configure content management systems and describe their applications in a residential environment.</p> <ul style="list-style-type: none"> Describe typical applications and physical connections of sources <ul style="list-style-type: none"> Media servers <ul style="list-style-type: none"> DVR Media PC <ul style="list-style-type: none"> Gaming systems MP3 players <ul style="list-style-type: none"> Satellite radio DVD players <ul style="list-style-type: none"> Legacy devices Satellite <ul style="list-style-type: none"> Streaming media Cable Summarize types of media storage, methods to transfer backup data <ul style="list-style-type: none"> Memory cards <ul style="list-style-type: none"> Local storage NAS devices (Network Attached Devices) <ul style="list-style-type: none"> Frequency of backup Remote storage Other connection considerations <ul style="list-style-type: none"> Digital Rights Management

Content sources

Explanation

In the modern home there are a wide variety of devices that members of the household might want to share over the home network. Being able to access these sources from various locations throughout the home is a goal many families would like to realize.

Media servers and media PCs



With lines between computers and other electronic devices becoming more and more blurred, there are dedicated devices that hold movies, music, and other A/V content for on-demand access. They usually contain large hard drives and connect to your home theater and HDTV system via digital cables. They connect to your cable or satellite feed and you can record the content for later access.

These devices are designed to provide a centrally located digital A/V system that can be distributed throughout the entire home. You can load the content of your CDs and DVDs to the server. It is then ripped and stored on the unit's hard drive for access later. You can access this through on-screen menus on your TV, on control devices throughout the home, and even on a networked PC.

Media Center editions of Windows XP and the Premium edition of Windows Vista include media server capabilities in a PC environment. Adding a TV tuner and surround sound system to the PC can enable you to enjoy the content on the PC. You can also send the data to your home theater and HDTV from the PC.

MP3 players

MP3 files are the most popular audio standard since WAV. The German company Fraunhofer patented it, and users must pay royalties for compressing files with it. With MP3 compression, computer users can compress the content of a music CD to one tenth of its original size. This allows up to 20 hours of music to be stored in one gigabyte of storage space. MP3 files are also streamable. This means that a computer can begin playing an MP3 file when only the first part of it is loaded in the computer's memory. It also allows an MP3 file to be sent over the Internet and played on the receiver's computer as soon as the head of the file arrives, while the rest of the file is still being transmitted.

Some audio receivers allow you to connect your MP3 player to them. In this way, you can access the content of your MP3 player over your home theater system.

DVD players

DVD technology offers crystal-clear pictures, superb multidirectional sound, massive data storage for computers and a host of interactive features such as selectable camera angles and a choice of movie endings. A majority of U.S. homes will soon have DVD players that convert the digital data recorded on a DVD to analog video that a non-digital television can display. These DVD player converters are now available for about \$100, a price that ensures that their popularity will continue to grow and that DVDs will rapidly replace VHS cassettes as the core of most home video libraries. DVDs are recorded in the MPEG-2 compressed format, allowing up to four hours of digital video to be placed on a single DVD. Quality is excellent, even though the playback for most users is still analog, and DVDs have now become the standard against which any other video compression format and display is measured for both picture and sound quality.

DVD movies are anamorphically encoded, which means that when a movie filmed in a wide-screen format is transferred to a DVD for home video viewing, the black bars that appear at the top and bottom of the NTSC (or SDTV) screen are encoded along with the movie. If the user has, or later gets, an HDTV digital receiver with a 16:9 aspect ratio, that television receiver can play the movie from the same DVD, but display the picture stretched out to fill the wide screen and eliminate the top and bottom bars. This ability of DVD technology to be forward compatible so that it can provide improved viewing on existing analog television equipment and still be compatible with more advanced digital technology added later by the consumer is one of the most appealing features of DVDs. It is made still more attractive by the fact that a DVD movie never wears out like VHS cassette tapes do after frequent viewing.

Satellite

Satellite broadcast relies on a dish antenna mounted to your home. The signal, broadcast from a geosynchronous satellite, is pure digital and reception quality is 100% or you will not receive an image. The only thing that will interfere with the signal is extreme weather such as heavy rain or snow. Usually reception is regained within a few minutes. Because the signal is digital the quality of the image is excellent. The dish feed is connected to a receiver, which decodes the signal and converts it for use on analog and HDTV sets. Each television you want to watch the satellite broadcast on requires a separate receiver.

Multi-switches are needed to split the incoming signal to go to each of the boxes for each television set. Some require power and some don't. They can combine both satellite and terrestrial antenna or cable signals saving you the need to run separate lines for each.

Diplexers allow you to combine the satellite signal and either a terrestrial antenna or a cable connection. This enables you to distribute both signals using a single cable.

Low noise block down converter (LNB) is the part of the satellite dish that converts the microwave signal from the satellite to a lower frequency band that the satellite receiver can use. This can be seen as the small object that extends in front of the dish in front of the lower portion of the dish.

Cable

Cable television signals are delivered locally over a mixture of fiber optic and coaxial cables. Signal quality has improved over the years and the service providers have added high definition service. Most cable providers require a set top box to unscramble the signal. The signal is often encoded so that only authorized subscribers have access to the broadcasts. Some content can be accessed directly without a set top box on cable-ready TVs. Unlike satellite, weather does not affect the delivery of the signal.

DVR

Digital video recorder (DVR) is also known as a personal video recorder. Brand names you might be familiar with include TiVO and ReplayTV. Computers containing TV tuners can also be used as DVRs. DVRs enable you to record content onto a hard drive for later viewing. It also enables you to pause and rewind live broadcasts and then return to viewing the live broadcast. Some satellite and cable provider companies include DVR capabilities in their set top boxes.

Gaming systems

Video game systems are popular among not only children and teenagers, but among many of the adults who first encountered them when game systems first came out in the 1970s. Game systems can be used locally without Internet access. Current game systems include the ability to connect to the Internet either via CAT5 or WiFi connections. This allows the players to play with anyone around the world. Some also function as CD and DVD players and as Web browsers. Some also function as MP3 players, photo viewers, and movies players as well.

Satellite radio

Satellite radio is a relatively new source for audio content. For a subscription fee, you can listen to the same station from anywhere in the United States. There are two satellite radio providers in the United States: Sirius and XM. They both have geostationary satellites located near the equator, so your antenna needs to be able to face south in order to pick up the signal.

Originally, the broadcasts were able to be picked up only on car radios equipped with XM receivers and antennas. As the popularity of satellite radio grew, they started making portable receivers. All receivers require an antenna that needs to face south to pick up the signal from the satellite. Some home theater components now include satellite receivers or enable you to connect your portable receiver to the home theater system.

Legacy devices

Do you remember eight-track tapes? This is an example of a legacy device. Other legacy devices include audio cassette tapes and many phonographs. Some audiophiles prefer the sound of phonographs over CD and DVD recordings, and have spent large amounts of money on high-end phonographs in recent years. Some performers do still record LPs as well as CD and DVD recordings. So, phonographs might be considered by some to be legacy devices, and not so by others. In general, analog devices are considered legacy devices and digital devices are not.

Streaming media

The Internet has a lot of content. This includes audio and video content. Audio content includes not only music, but also radio stations, archived broadcasts of shows and performances, podcasts, and satellite radio content. Some of the content is available for free; others require subscription or per-item fees.

Some content is available as downloads only. This places a copy of the content on your local storage device. Other content is streaming content, which does not place a copy of the content on your local storage device. The streaming content is played as you are listening and/or watching it be delivered to your computer.

Internet radio stations can be listened to over the Internet. This allows you to hear your favorite stations no matter where you are as long as you can connect to the station's Web site. Some radio content is archived and then you download it to your storage device for listening at your convenience; in this case, it would not be streaming audio.

Podcasts are downloadable files. These can be archives of radio shows, or they can be content that is strictly available in the podcast format. The Web site podcast.net is a directory to which users can add their podcasts.

Video content includes news video footage such as the content you might find on MSNBC. YouTube.com is a popular Web site that includes video footage shot by people all over the world who want to share their videos with anyone and everyone. It is also possible to download full length movies from various sites.

Be aware, however, that not all of the content you find on the Internet is there legally for your download and use. Some of the content is public domain or not copyrighted. However, there is a large community of Internet users who ignore copyright and post the content for access by others.

Do it!

B-1: Identifying content sources

Questions and answers

- 1 Which of the content sources would you include in your home theater system? Why?

Answers will vary based on the needs of the user, but might include media server, media PC, MP3 player, DVD player, satellite and/or cable connection, gaming systems, or other legacy devices

- 2 Which versions of Windows XP and Windows Vista are designed for serving media content to a home theater system?

Windows XP Media Center edition and Windows Vista Premium and above

- 3 Which of the content sources require a monthly subscription fee?

Satellite TV, satellite radio, cable TV, some music and video download Web sites

Media storage types

Explanation

Storing your audio and video files takes up a great deal of room. Most PCs and media servers contain hard drives of at least 200 GB and usually even larger. However, this is not always enough storage space. In most cases you can simply copy the content from one location to another. For some storage types, you need to use a network protocol such as FTP in order to upload or download content. If you are downloading the file from the Internet, you will need to go through the Web browser to access and download the content.

Memory cards



If you have examples of various memory cards, share them with students.

Sometimes you don't want or need to transfer audio or video images from their native storage medium to the hard drive of your media server or your computer. For example, if you are viewing the images from your digital camera on your HDTV, you might just want to connect the camera or insert the media card into the Media PC or Media Server if it has the proper slot for the card without transferring the images to the hard drive. These memory cards, also known as flash memory, come in a variety of formats. CompactFlash cards are quite common. Others include SmartMedia, xD-Picture Card, Secure Digital (SD), MultiMedia Card (MMC), and Memory Stick and Memory Stick Duo. Some of these flash media types are also used in MP3 players to hold music and can be connected to your home theater system for playback. Some examples are shown in Exhibit 3-5.

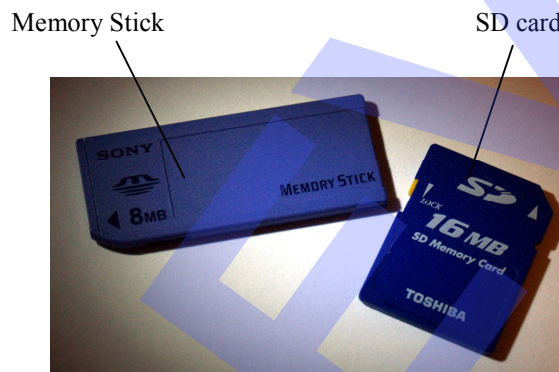


Exhibit 3-5: Memory Stick and SD flash memory cards

Digital video cameras record on MiniDV, Digital8, DVD, or flash memory cards. These typically capture and play back in SDTV resolutions. High definition video cameras have become available now and record in either High-Definition Video (HDV) format or Advanced Video Codec High Definition (AVCHD) format. HDV uses MiniDV tapes. AVCHD usually writes to a miniature DVD. The AVCHD disks can be played in Blu-ray disc players.

NAS

Network attached storage (NAS) devices are typically found in the business world to provide additional storage for network servers. In the home environment, they can also provide you with additional storage space for audio and video content. These devices connect directly to the network rather than to a computer. The NAS device has a built-in operating system.

Remote and local storage

Remote storage makes use of space on an Internet server for you to store and share files. It is designed to function just like your local computer storage. Some services provide a small area for free to users; then, if you need more space, you can pay an additional fee to lease more storage space. Files might be uploaded to the remote storage location by using a custom interface or you might need to use protocols such as FTP to upload files.

Local storage refers to any of the drives or media storage devices that are located on the premises. These are typically attached directly to a MediaPC or Media Server. Sometimes, for example with a flash memory card, they can be inserted directly into a viewing device on your home theater system.

Backups

Once you have put several hours of content on your media server, you should create a backup of the server in case something should happen to it. If you purchased and downloaded a movie from the Internet, you don't want to lose it. Traditionally, hard drives were backed up to tape drives of one sort or another. Many users now connect an external hard drive via USB or IEEE 1394 (also known as iLink or FireWire) connections and simply copy the data to a second location.

It isn't necessary to copy all of the files every time. If you are using a backup utility, there should be options to perform a full backup or a partial backup. The partial backup copies only those files that were changed or added since the previous backup. If you are just copying files to the second drive, you will need to keep track of which files were added or changed and copy those files manually when you want to create a backup.

Do it!

B-2: Discussing media storage types**Questions and answers**

- 1 Compare local and remote storage.

Local storage refers to any of the drives or media storage devices that are located on the premises. These are typically attached directly to a MediaPC or Media Server. Local storage might include memory cards, additional disk drives, and NAS devices. Remote storage is located on a server at another location and there is often a fee for using the space on the server.

- 2 How do you transfer data between storage devices?

You can usually simply copy the data. Other times, you will need to use network protocols such as FTP or IP downloads.

- 3 You added a new movie to the media server. Do you need to back up the entire server again to get a good backup that includes the new movie? Why or why not?

You can do a partial backup or if you are creating backups by copying the files to another location, you can just copy the new movie to your backup location.

Digital rights management

Explanation



Digital rights management (DRM) technologies are used to control both use and access of digital content and the hardware on which the content is accessed. It also refers to the restrictions placed on a specific piece of digital content. DRM are designed to protect the content for copyright holders.

Copy protection and technical protection measures are the technologies used for access control to digital content. These are components within a DRM.

The manufacturer of the discs or the downloadable content might include special encoding of the content that prevents you from copying the material or from accessing it more than a certain number of times. They might also set an expiration date on access to the content. Others enable you to copy the content to up to a certain number of devices.

One example of DRM is used on the songs downloaded from the iTunes Store, which have an encryption method called AAC. This allows the songs to be played on iPod devices and burned to CD. They cannot, however, be copied to other MP3 players.

Sony developed software that would prevent a CD from being copied more than a certain number of times. However, they did not make it known that this software would be installed on computers. The courts ruled this unacceptable and Sony was forced to replace the CDs with copies that did not include this rootkit software.

Do it!

B-3: Considering digital rights management

Questions and answers

1 Using your Web browser, locate an article that discusses digital rights management. Determine what their stance is on the issue. Share your findings with your classmates.

2 When is it acceptable to download copyrighted music from the Internet?

When you have been given permission by the manufacturer. This might be by paying a fee or they might identify certain pieces of music as freely downloadable.

3 Explain the relationship between copy protection, copyright, and DRM.

Copy protection is a method of protecting the copyright holder through DRM.

Topic C: Implementing multi-room audio/video systems

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
2.2	Install, configure, and maintain a residential home theater system. <ul style="list-style-type: none">• Audio components<ul style="list-style-type: none">• Audio/video components setup and integration• Video components
2.4	Implement, maintain, and troubleshoot multi-room video systems. <ul style="list-style-type: none">• Define signal types and their applications<ul style="list-style-type: none">• Digital distribution (for example, analog to IP converters, IP to analog converters, wireless distribution, IEEE 1394)• RF distribution characteristics. Identify and troubleshoot noise and interference (for example, splitters and taps, active and passive, attenuation, bi-directional, modulation and filtration, amplification, IR over coax)• Analog distribution (for example, composite, component, and S-video, balun)• Identify cable types and their applications<ul style="list-style-type: none">• Coaxial (RG-59, RG-6, RG 6 QS, DV, serial data, CCS, BC)• Cat5/5e/6• Termination (RCA, BNC, F)• Satellite<ul style="list-style-type: none">• Multi-switches• Diplexer• LNB (Low Noise Block Down) converter

Setting up an audio system

Explanation

When you set up an audio system, you need to consider how it will be used as well as the space in which it will be installed. The components you choose to install will vary with both of those considerations. Your budget will also affect which options you choose to set up.

Do it!

C-1: Setting up audio system components

Here's how	Here's why
1 Locate the amplifier	You will set up an amplifier and connect the speakers to it by using the appropriate cables.
Place the amplifier in the location where it will be used, making sure you have access to the rear panel	If you are placing the amplifier in a cabinet, make sure there is ample air flow around it.
Determine the speaker connection options on the amplifier	You might have optical connectors or two conductor speaker wire connectors that connect using a clip, a screw-down device, or banana plugs.
2 Locate the front left and right speakers	Be sure to place them in the appropriate locations relative to the listener.
Determine the type of connectors available for connecting the front speakers	
Connect the speakers to the amplifier	
3 Locate the center channel speaker	
Connect the speaker to the amplifier	
4 Locate the rear left and right speakers	
Connect the speakers to the amplifier	
5 Locate the subwoofer	
Connect the subwoofer to the amplifier	This might use a different cable and connector type than the other speakers use.
6 Plug the amplifier into the power source	You might consider plugging it into a surge strip to protect the equipment.

Cable types

There are several types of cables that are used when implementing a multi-room video system. These include coaxial cables of varying thicknesses. The data on coaxial cables is carried in a serial fashion: one bit after the other rather than several bits side-by-side.

Coaxial

Coaxial cable thicknesses are rated by the type and thickness of the core wire. The designations begin with RG, which stands for Radio/Government. RG-59 cable is used for standard cable TV connections. RG-6 largely replaces RG-59 cabling. It has an 18-gauge copper core and is either double or quadruple shielded. The quadruple shielded version is also known as RG-6 QS. Both RG-59 and RG-6 have 75 ohm impedance. BC or bare copper cables have had the shielding removed so that the proper terminator or connector can be applied to the cable.

The inner conductor wire in a coaxial cable is typically composed of *copper clad steel* (CCS). This is a wire that blends together the conductive properties of copper and the resistance of steel.

Cat 5/5e/6

The Cat 5 and higher cabling used in your home network can also be used to connect your video system between rooms. You will need baluns to convert the signal between the connector type used on the video equipment and the network cable and then back to the cable type on the video equipment in the remote location.

Do it!

C-2: Setting up video system components

Here's how	Here's why
1 Place your TV so that the cables can reach your amplifier and other local home theater system components	You will set up the video components of a home theater system.
2 If you are using a SDTV, connect the TV to the amplifier by using RCA cables If you are using an HDTV, connect the TV to the amplifier by using DVI or HDMI cables	
3 Connect the TV to the remote broadcast source	This might be a satellite box, a cable box, or a terrestrial antenna.
4 Connect a DVD player to the amplifier Connect the DVD player to the TV	This connection might be made using RCA, optical, or HDMI cables. This connection might be made using S-Video, DVI, HDMI, or RCA cables.
5 Connect the TV to the power source	
6 Connect the DVD player to the power source	

Configuring audio/video system components

Explanation

Now that you have set up all of the A/V components, you need to configure them to get the best output from them. You can use automated setup tools or you can manually adjust settings as discussed earlier.

Video setup

Just because you bought a high end video system doesn't mean that it will look as perfect as it did in the store when you bring it home and set it up. It might, but it might not. If you want to adjust the setup, there are several calibration settings you can change. The set is probably configured to automatically calibrate what it deems to be the best image. If you want to change this, you will need to change from automatic to manual or professional mode.

There are calibration discs that you can purchase. These contain hundreds or thousands of images that can be viewed as you make and test the changes.

The first setting to adjust is brightness and contrast. Turn the color all the way down until you have a black and white image. Adjust the set's brightness control to make the black as dark as possible. You can then adjust the contrast so that you can see faint differences in very dark areas of the image. Next, adjust the color control for proper color level.

Then adjust the tint control for flesh tones. If you use calibration discs, they will help you through the process. While this setting is a matter of personal preference to some degree, you don't want people to have orange or green faces.

Adjust the sharpness control next. This is also a subjective adjustment to some degree. Setting the control too soft will result in a fuzzy picture. Setting it too high will result in ghosting of the images.

Audio setup

It is important that you read and follow the directions for fine tuning the system. Some have an automatic setup to adjust the speakers once you have them placed and wired. Such a setup automatically adjusts the volume output from each speaker along with the time delay from each speaker based on the listening position. Others will use a more hands-on approach to tuning the system.

*Do it!***C-3: Configuring audio/video system components**

Here's how	Here's why
1 Turn on the TV and the amplifier	You will configure the A/V components that you installed previously.
2 Tune in a station on the TV Verify that the picture is displayed correctly and that the sound is being played through all of the speakers	
3 Determine if you think the TV set needs to be calibrated If necessary, calibrate the TV	This is a personal preference in most cases. However, if the set is obviously showing green faces or ghosting or some other problem, you will need to calibrate it. You should start with automatic calibration options if possible and switch to manual mode if the automatic option does not correct the problems.
4 Determine if the audio system is correctly balanced If necessary, rebalance the system	Again, this is usually a personal preference. However, if some of the speakers are overpowering others, you should rebalance the system. Refer to the documentation that came with the amplifier for how to balance your particular system. Most have an automatic balancing method. If not, it should provide you with detailed step-by-step directions for how to balance it.
5 Turn on the DVD player	There is not usually any configuration required for this component.

Testing A/V system components

Explanation

Now that you have set up and configured your home theater system, you can test it. Try playing various types of music and movies. Each might require a slightly different calibration or balance, but rather than adjusting for each of those variances, most users adjust it to accommodate all of the types of audio and video with a single setting. Some systems do allow you to save settings for multiple preferences, which you then select through a menu.

Do it!

C-4: Testing audio/video system components

Here's how	Here's why
1 Insert an audio CD in the DVD player	You will verify that the audio and video component perform to your satisfaction by trying several different types of music and movies.
Play the CD	
Determine if you would prefer a slightly different balance	
Determine if you would prefer a slightly different speaker placement	Try moving the front left and right speakers nearer to the wall or further from the wall and see if you can hear a difference.
2 Try moving the subwoofer to another location	For example, if you played a hard rock CD first, try a CD of ballads now.
Do you notice a difference? Do you like the original placement or the new placement better?	
3 Play another CD with a completely different sound	How you do this will vary among equipment.
4 Insert a movie in the DVD player	
On the TV, select the appropriate video input for the DVD player	If so, make any necessary adjustments.
5 Verify that the DVD is playing on the TV	
Do you notice any problems with the signal from the DVD player?	If the first movie had a lot of dark scenes, try to find a brightly lit movie for this test.
6 Try another movie	
Determine if you would make any changes in the TV to view the movies	

Explanation**Digital distribution**

Distributing A/V signals over digital cables and equipment enables you to reach further than you would be able to send the signals using standard speaker wires with minimal or no noise or interference issues. In order to do this, you need to convert between analog and digital signals.

Analog to IP converters

Analog to IP converters are used to convert analog audio/video signals to a digital format. The digital signal can then be sent over the network by using the IP protocol. This enables viewing of images remotely over Cat5 cables and even the Internet. The converter integrates analog equipment such video cameras and allows them to be used in a digital system.

IP to analog converters

Digital to analog converters are used to integrate digital signals into existing analog environments. This allows a mixture of both analog and digital signals within an A/V system. They convert a digital feed to be able to be viewed with analog TV and video recording technology.

For example, there are units that convert single link DVI-D signals to analog RGB signals. This enables you to easily integrate digital video sources into conventional analog systems.

Wireless distribution

If the device you are sharing is capable of wireless network connections, you can share the digital content over your WiFi network. Wireless receivers can be set in any and all rooms to access the information. Examples of such wireless devices might include Sony PSP devices, some security cameras, and wireless headsets.

You can also connect wired devices to a wireless media streaming device that can then broadcast the wireless signal to other devices throughout the home. For example, you can take signals from sources such as computers, cable or satellite set top boxes, and DVD and VHS players. The signals are taken into the box via the connecting cables, and then sent out via wireless networking standards. The signal can be sent out to other computers, projectors, video monitors, and TVs that have been set up with wireless receivers.

IEEE 1394

Digital video cameras include the IEEE 1394 connection. This is also known as FireWire or iLink. You can share the images from the video camera by connecting it to a device on the network that is capable of sharing content. Most computers and most HDTVs include this type of digital connection.

RF distribution

RF distribution devices have been used to share signals between rooms in hotels, hospitals, schools, and apartment complexes. This same technology is available to enable you to share signals between rooms in your home. You are familiar with the cable outlet that the cable company runs into your home. Each room may be wired for an outlet with the use of amplifiers and splitters to split the feed and keep the signal strength for a quality feed.

Splitters and taps

A splitter divides the signal into equal portions to share between the rooms. Some splitters are powered. These are referred to as active splitters. With an active splitter there is no loss of signal when the feed is split. A passive splitter is not powered and there is the potential for signal loss when the feed is split. This loss of signal strength is referred to as *attenuation*. The signal is amplified when using active splitters, but it isn't amplified when using passive splitters.

A tap doesn't split the signal equally. It causes only about a 1 dB loss in the cable and a 6 to 12 dB loss at the tap. This compares to about a 4 to 5 dB loss at each output on a splitter.

Modulation and filtration are used for channel selection and noise filtration. Noise shows up as static or a hum. You will likely get more noise on a low quality splitter or tap.

A bi-directional RF distribution device not only allows you to share the output between various locations, but it also enables the users to send information back to the source. This enables users to access pay-per-view channels and interact with cable content. It also is part of the technology involved with cable modems.

IR over coaxial

IR coaxial adapters enable a signal from a universal remote to be picked up and transmitted to the media server over a coaxial cable. The signal is sent to an IR emitter at the media server to rebroadcast the signal from the coaxial cable as an IR signal.

Analog distribution

Analog video signals include composite, component, and S-Video. A balun can be used to connect any of these signals to a CAT5 distribution network as long as the balun has the appropriate connector type for the analog connection. Analog signals include composite video, component video, and S-Video.

Composite video

Composite video is carried on the yellow color-coded RCA cable. It is the video portion of an analog broadcast signal. Composite video consists of three source signals:

- Y is brightness or luminescence
- U and V carry color information

Component video

Component video is the composite video that has been split into three separate signals. This provides a higher quality signal than composite.

Component video connectors use three RCA connectors to send a brightness signal and two color signals. The three connectors are labeled red, green, and blue. Together they provide a higher-quality signal to the television than can be obtained with either a composite or S-Video signal. Component video connections sometimes use BNC connectors or the VGA-type connector used for component connections on computers. All component video connections use separate wires for audio in addition to the three video signals.

S-Video

S-Video (separated video) is another type of video connection that does not combine the entire video output into a single signal, but leaves it as separate brightness and color elements that are sent by separate wires (along with separate audio wires) in the output connection. S-Video is also an analog video output, like composite output, but it provides better quality than the composite signal.

Do it!

This is written to use the X10 Model VK80A A/V Sender and Receiver. If you use another multi-room option, adjust the steps accordingly.

C-5: Setting up a multi-room wireless A/V system

Here's how	Here's why
<p>1 Connect the RCA cables from the TV audio and video lines out to connections on the wireless transmitter</p> <p>Set the channel selector on the transmitter to Channel 3</p> <p>Connect the transmitter to a power source</p>	<p>You will set up a wireless RF distribution system to share signals between two TVs.</p>
<p>2 Connect the wireless receiver to the second TV by connecting the RCA cables from the receiver to the audio and video lines in</p> <p>Set the channel selector on the receiver to Channel 3</p> <p>Connect the receiver to a power source</p>	
<p>3 Adjust antennas so that they face each other</p>	<p>To achieve optimum reception such as eliminating noise in the signal. Even if the signal is in another room, the antennas need to face each other to get the best possible signal.</p>
<p>4 Refer to the documentation to configure the IR remote control to recognize your TV</p>	<p>The documentation that comes with the remote control will have codes that you enter for each brand and sometimes for the model of equipment you are trying to control.</p>
<p>5 Using the remote control, change the channel on the TV receiving the signal</p> <p>Determine whether the TV sending the signal also changed channels</p>	

Unit summary: Audio/video system concepts

Topic A

In this topic, you learned about **home theater system components and characteristics**. First you learned about **acoustics** basics, including **sound reflection**, **speaker placement**, **sound cancellation**, and **sound balance**. You also learned about proper **cable use** and the difference between **line levels** and **speaker levels**. Next, you examined amplification, including **Ohm's law** and **local and centralized amplification**. You also learned about **multi-channel sound** concepts, including **crossovers**, speaker setup, types, and **surround sound numbers**. Next, you examined **types of speakers**; **single, multiple and local sources**; and **speaker specifications**. You learned about video display types, including **CRT**, **flat panel**, and **projection systems**. You also learned about tuner types such as **NTSC** and **ATSC**. Next you learned about **video processing** and **digital video cables**. Finally, you learned about **MRAV standards** and control devices.

Topic B

In this topic, you learned how to identify **content management systems** and how they are used in home theater systems. First you learned about content sources including **media servers and PCs**, MP3 players, DVD players, satellite radio and TV, cable, DVR, gaming systems, legacy devices, and streaming media. Next, you learned about memory cards, NAS, remote and local storage, and backups. Finally, you examined the issues surrounding **digital rights management**.

Topic C

In this topic, you set up and configured **multi-room audio and video systems**. First, you examined how to set up audio and video system components. Next, you configured and tested the A/V components. Finally, you identified methods of A/V distribution and set up a wireless RF A/V distribution system.

Review questions

- 1 List some of the multi-room audio system control devices.

Keypads, rotary volume controls, sliders, push button controls, touch screen, wireless keypads, and handheld devices

- 2 Compare direct view and projection displays.

LCD, CRT, and plasma are direct view displays. DLP and LCoS are projection displays.

- 3 Compare composite, component, and S-Video signals.

Composite video is carried on a single RCA cable. Component video is carried on three separate cables. S-video sends brightness and color on separate wires and is the highest quality of these cable types.

- 4 _____ technologies are used to control both use and access to digital content and the hardware on which the content is accessed.

Digital Rights Management

- 5 List some of the media storage types.

Memory cards, NAS devices, remote and local storage

- 6 What is the difference between regular RG-6 and RG-6 QS cable?

The regular has dual shielding and the QS has quad shielding.

7 What is crossover in terms of speakers?

Crossover identifies the frequency at which signals switch between mid-range, LFE, and tweeters.

8 Why is it important to match impedance?

To prevent overheating and damage to the amplifier.

Independent practice activity

You will design a three room home theater system. The first room is 12×24 feet with a fireplace on the short wall and a window behind the three recliners that will face the TV in the family room. The additional rooms are a basement children's activity area and the master bedroom. It will include:

- A rear projection HDTV in the family room
- An LCD television in the children's area
- A plasma television in the master bedroom
- DVD
- Phonograph
- Satellite radio
- Cable TV
- 7.1 surround sound

- 1 Determine where the source equipment will be located.
- 2 Determine how the equipment will be connected.
- 3 Show the placement of speakers in each room and determine if you will use any in-wall or in-ceiling speakers.
- 4 Identify any acoustic issues you will need to consider in any of the rooms.

PREVIEW

NOT FOR PRINTING OR INSTRUCTIONAL USE

Unit 4

Telephony and VoIP

Unit time: 90 minutes

Complete this unit, and you'll know how to:

- A** Describe POTS delivery and troubleshoot common issues.
- B** Describe VoIP delivery and troubleshoot common issues.
- C** Describe and define fundamentals of telephone systems.

Topic A: Plain Old Telephone Systems

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
3.1	Differentiate and describe POTS vs. VoIP delivery. Identify and troubleshoot common issues. <ul style="list-style-type: none"> • POTS <ul style="list-style-type: none"> • Crosstalk • Radio Interference • Dead Ports • REN (Ringer Equivalence Number)

Analog telephone communication systems

Explanation



What we know as *Plain Old Telephone Service (POTS)* is an analog system of phone lines and equipment. Even today, some 40 or more years after the introduction of digital voice transmission, most home telephones are still analog devices connected to analog phone lines. Once the phone line reaches from the home to the nearest telephone exchange, it likely connects to a digital transmission line, but the local “last mile” of phone line from the telephone exchange to the typical residence is usually still analog.

As the need for more and faster communication has accelerated in recent decades, the analog phone system has been taxed to provide the necessary service. Analog signals move relatively slowly when carried in physical media such as copper wire and cable. Telephone voice transmission signals travel at speeds from about 300 Hertz (Hz: cycles per second) to 3,300 Hz. Although this might seem relatively fast when compared with, for example, the speed of an electric motor, it’s downright snail-paced when compared with digital data speeds over a network, which are measured in millions of Hertz (MHz), or wireless data transmissions, which are measured in billions of Hertz (GHz).

Analog voice communication signals are also subject to weakening due to resistance in the wires through which they travel and to *interference* (noise) caused by electrical equipment, power lines, and even some electric lights. In a telephone conversation, this noise is heard as static on the line. The weakened signal of an analog transmission must be strengthened periodically by an amplifier. Unfortunately, an amplifier can’t separate noise from the voice part of the signal, so it amplifies both. Voice conversations that have been amplified several times usually can still be understood, because the human hearing system is very adept at extracting the correct meaning of spoken words from background sounds. Data transmissions sent over analog lines don’t always fare as well, because the data is interpreted by machines that don’t “hear” as well as people do. The result is that noise in analog data transmissions frequently causes errors.

Data transmission using analog modems is limited to about 56,000 bits per second when receiving data and about 33,000 bits per second when sending data. The analog public switched telephone network (PSTN) operates at 2,400 baud. A baud is one complete cycle or wave in a transmission signal. A baud starts at zero voltage, goes up to maximum positive voltage, comes back to zero, goes to maximum negative voltage, and finally returns to zero voltage. A 2,400-baud line carries current that completes 2,400 of these wave cycles each second. The baud rate refers only to the frequency of the current. It doesn't indicate the amount of data that's transmitted on the line. A 56,000-bit modem uses technology that allows it to put 24 bits of data on each wave of a 2,400-baud line (56,000 divided by 2,400 = 24). The line current is still running at 2,400 baud even though 56,000 bits of data per second are being transmitted on it. That's about the limit for an analog data line, however. To send more than 56 Kbps of data requires a shift to digital transmission technology.

Voice and data can both be sent on an analog line at rates up to the limits that analog lines can transmit. Within a home, the requirements for voice communication by telephone almost never exceed the limits of analog technology. Frequency division multiplexing even allows analog lines to carry multiple conversations or data streams simultaneously. This feature is accomplished by dividing the available analog frequencies on a line and sharing them among various voice and data transmissions. Thus, one voice data stream might be running on a line at 2,400 baud, while a second is running at a higher baud rate and a third at a still higher rate. Multiplexing allows multiple telephone lines to be installed in homes and businesses without the need to install additional wiring from the telephone company office to the home.

If voice links were all that were required of phone lines, analog alone would probably be sufficient, at least within the home. But most homes now also require data transmission over the same telephone lines that handle conversations on the telephones. If the phone lines are even occasionally filled by analog voice transmissions, which can't be delayed or interrupted without interrupting or garbling a real-time conversation, they can't meet additional data transmission requirements.

To have enough capacity for the system to handle both voice and data needs, additional lines must be installed, or the capacity of the existing lines must be increased by transmitting digital data on them. Not only must the data be sent digitally, but the voice transmissions must be sent digitally as well. If either were left in analog form and sent with that technology, they would consume so much of the line's capacity that there would be insufficient capacity left for the digital transmissions.

Changing both voice and data transmission to digital format provides a huge increase in capacity for a telephone line. The majority of homes are still using analog lines for telephone voice transmission and for data lines that connect analog 56 Kbps modems to ISPs, but the shift to digital transmission lines that can carry anywhere from three times to dozens of times the data of an analog line is accelerating. The demand for increased data transmission rather than additional voice lines is driving this transition.

*Do it!***A-1: Defining POTS features****Questions and answers**

1 Telephone voice transmission signals travel at what speeds?

From about 300 Hz to 3,300 Hz

2 What factors weaken analog voice communication signals?

Resistance in the wires and interference

3 Explain why an analog PSTN at 2,400 baud can transmit data at 56,000 bits per second.

A 56,000-bit modem uses technology that allows it to put 24 bits of data on each wave of a 2,400-baud line (56,000 divided by 2,400=24).

Telephone installation and configuration

Explanation

Since telephone service began the equipment used has continually increased in complexity and capacity to meet the demands of users. Looking back, it's easy to see with perfect hindsight that early wiring and infrastructure didn't provide for nearly enough future expansion. This is especially true in residential telephone service where single line analog telephone service wired with two-wire telephone line is the norm. Wiring and installation of telephone systems today should benefit from past experience and provide not only for more capacity than is currently needed, but also for more than current technology levels suggest will ever be needed. Experience has shown that the use of data transmission systems (telephone, network, radio, and television) has continually increased at a pace that far exceeded the most optimistic predictions. There's no reason to think that home telephone service ten years from now won't need a hundred times the capacity it needs now.

Telephone equipment is wired and installed in much the same manner as network and other electronic equipment. The same care should be taken in wiring to use adequate cabling and install it to standards, make data-secure connections, and test systems carefully to be certain that they function correctly.

There are literally thousands of devices available for use in home telephone networks. This section discusses only a few of the basic installation procedures that you need to know for all home systems. The installation instructions for any telephone system device should always be studied and followed precisely to ensure that the individual requirements of the equipment are met.

Connecting telephone equipment

Analog telephones have long been wired with cable consisting of two or four copper wires. The wires are single strand and aren't twisted into pairs. A single telephone line requires only two wires, and so a four-wire cable could connect two lines. Because the wires aren't twisted, crosstalk interference was common. Persons speaking on one telephone line could often hear a low-volume background conversation, which was usually someone talking on the other line. Exhibit 4-1 shows an old-style wiring block wired for two lines. The round four-wire cable, secured with staples, can be seen coming in from the right side of the photo. The individual wires lead out to an extension phone above the block but not visible in the picture.

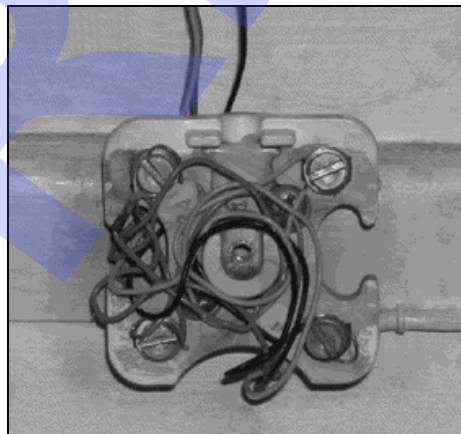


Exhibit 4-1: An old-style telephone block wired for two lines

This old-style wire has a color code that's slowly disappearing in favor of the color coding used for twisted pair cables that connect high-speed data networks. The following table shows this older wiring color scheme for a four-wire or a six-wire cable. This color code is still important to know, as you'll likely encounter many existing telephone systems still wired with it.

Wire pair	Wire 1 color	Tip/Ring	Polarity	Wire 2 color	Tip/Ring	Polarity
1	Green	Tip	Positive	Red	Ring	Negative
2	Black	Tip	Positive	Yellow	Ring	Negative
3*	White	Tip	Positive	Blue	Ring	Negative

**The third wire pair is applicable only to 6 wire cable.*

The designations “tip wire” and “ring wire” come from the old ¼-inch phone plugs that were used to connect phone lines in operator-run PBX boards. Each jack connected a phone line and so had two wires running from it. The tip wire was the positive wire and was connected to the tip of the plug. The ring wire was the negative wire and was connected to the ring or side of the plug. This traditional designation has remained in use even though its original meaning no longer applies.

The old color code is now being replaced by one easier to remember. It's shown in the following table.

Wire pair	Wire 1 color	Tip/Ring	Polarity	Wire 2 color	Tip/Ring	Polarity
1	Blue/white	Tip	Positive	Blue	Ring	Negative
2	Orange/white	Tip	Positive	Orange	Ring	Negative
3	Green/white	Tip	Positive	Green	Ring	Negative
4	Brown/white	Tip	Positive	Brown	Ring	Negative
5	Slate/white	Tip	Positive	Slate	Ring	Negative

There are additional pair colors for this color code, as there were for the older one, but home telephone systems aren't likely to use cables with more than five pairs of wires.

Today, telephone wiring is installed using twisted pair cable. Category 5 cable is the new standard for analog telephone lines. Basic telephone wiring isn't difficult but should be performed carefully to ensure good connections and that lines meet their data transmission requirements.

Pulling Cat5 or similar cable for telephone connections should be done using the same techniques and following the same cautions as cable pulled for a network. Even though the data transmission requirements for the telephone lines may not be as high as for the data lines, installing the cable with the same (maximum) adherence to standards ensures that it performs with peak efficiency and can be used in upgraded systems with higher data requirements later.

RJ-11 connections

The Bell System telephone company developed the Universal Service Ordering Codes (USOC), specifying the wiring configurations for the series of Registered Jack (RJ) types used to connect residential telephone equipment to the public network. Exhibit 4-2 shows these wiring configurations for one line, two lines, three lines, and four lines. An RJ-11 jack is the standard single line telephone connector. An RJ-14 jack is the standard two-line connector.

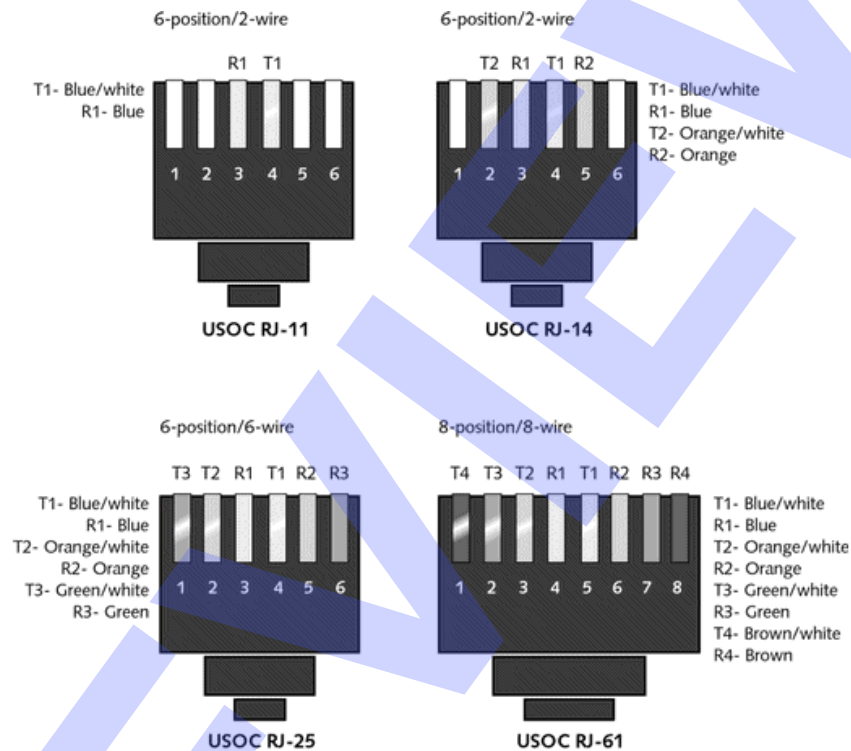


Exhibit 4-2: Telephone plug and jack wiring standards

These color codes for telephone wiring differ from those used for RJ-45 jacks and plugs, but the procedures for terminating cables to jacks and plugs are the same. Wires must be set in the plug according to the color pattern shown in Exhibit 1-5, but all the other steps in the terminating process are the same. Wires not used in a multiple-pair cable when terminating it to a jack or plug should be cut off at the plug or jack entrance, so that they don't interfere with connected wires or produce short circuits in the cabling.

Exhibit 4-3 shows some of the major parts used for wiring telephone lines. Moving clockwise from the upper left, the photo shows an RJ-11 plug, a 4-pair wire, a splitter for doubling extensions from an RJ-11 plug, and an RJ-14 4-wire jack with its cover removed.

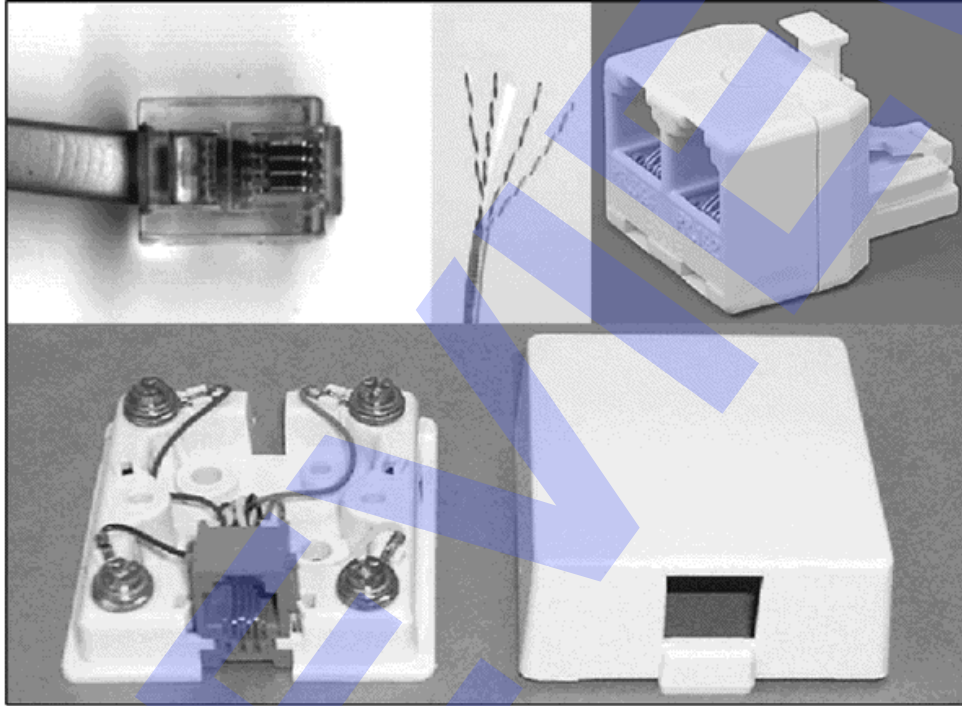


Exhibit 4-3: Telephone wiring components

If wiring is being installed for a network and for telephone lines, a single Cat5 or similar cable can be used to accomplish both connections. Only two of the Cat5 cable's four pairs of wires are used for network connections. The remaining two pairs can each be used to wire a telephone line in a combination jack. If one cable is used for both types of connections, the RJ-45 jack must be wired using only the two pairs of wires actually needed for the data connection. The other two pairs aren't included in the jack connection but are left free to be wired to an RJ-11 or RJ-14 jack as telephone connections.

The colors of the pairs that must be used for the telephone lines don't follow the USOC standard but are one or both of the twisted pairs not used for the 2-pair data connection. You must keep careful track of which pair is used for each telephone line and connect the lines identically at both terminations.

Fax machine communications

Fax machines are digital devices that operate on analog telephone lines. The analog telephone line's capacity limits the speed of a fax machine to about 54,000 bits of data per second and, at this speed, some errors in data transmission are likely.

When sending or receiving a document, a fax machine uses the full capacity of a telephone line. No simultaneous voice transmission is possible on a standard analog line. Because fax machines don't usually operate constantly, especially in home environments, this means they can usually share a telephone line that's used for voice calls when not occupied by a fax transmission. Many fax machines are designed for this type of line sharing. They have built-in circuitry that determines whether an incoming call is a fax transmission or a voice call. If it is a fax message, the machine activates to receive and print it. If not, it allows the call to ring the attached telephone, so that the voice call can be answered.

Modem communications

For those homes that are not using broadband cable or DSL connections, their computers are typically connected to the Internet through a modem. The modem is usually installed as a card inside the computer, although some are external devices that connect through the COM (serial) port on the computer.

Whole house distribution

You can use splitters to add additional phone jacks in various locations throughout the house. Another method of having phones available throughout the house is using portable phones. Some portable phone systems are available in which only the main base station needs a phone line connection. Other phones (usually between two and seven additional phones) communicate with the base station over 900 MHz or 2.4 GHz radio frequencies.

In most cases, you need to install a jack in each location where you want to place an additional phone. However, some multi-phone systems communicate with a base station, which is the only component of the system connected to a phone jack. In this system, the handsets for the additional phones are charged in remote cradles and communicate with the base station over the 2.4 GHz band.

Do it!

A-2: Setting up and configuring POTS access

If the building uses digital phone lines, be sure not to plug an analog phone into the port.

If you want, you can have students send or receive faxes to each other.

This step is optional if you don't have an ISP to which they can connect.

Here's how	Here's why
1 Determine the connector type on your telephone Verify that it is the same type of connector as the phone jack	You will connect a telephone, a fax machine, and a modem to a phone line.
2 Insert a phone line splitter into the jack Connect a phone cable to each connector port	This enables you to connect more than one telephone line to the port.
3 Connect a telephone to one cable Connect a fax machine to the other cable	
4 Verify that the phone has a dial tone	Lift the receiver and you should hear the dial tone, which indicates that the line is available for placing a call.
5 Following the directions with the fax machine, configure it to accept and send calls	If it has the ability to determine if a fax transmission is incoming, configure that to pick up on the second ring.
6 Locate the modem in your computer Unplug the cable connected to the phone and connect it to the Line port on the modem	It is probably internal and is identified by the RJ-11 jack on the card. It might be an external device that needs power supplied to it and a phone cable connected to it. You can still have the phone connected by using another phone line and connecting between the phone and the phone port on the modem.
7 Following your instructor's directions, configure the modem to dial a local ISP Connect to the ISP Disconnect after making the connection	

Explanation**POTS issues**

Phone technicians use network tone generators and butt sets to check the lines and extensions on the phone system. Using these tools, they can determine if the problem is at the phone, with the line or the jack, or at the main system.

The ports to which handsets or other devices are connected might fail. This is referred to as a dead port. If you use a connection block or patch panel to connect multiple phone lines to a trunk cable to the telephone company's lines, this is usually located on the outside of the house. Sometimes if you have a large phone system, it might use cards to add additional connections. Any one of the ports to which devices connect can go bad. These dead ports are usually not repaired, and the card is replaced or another open port is used.

REN

Ringer Equivalency Number (REN) is a method of determining the load a device will place on a phone line. In the United States, the line can support a REN of 5. In the United Kingdom, a REN of 4 is supported. Other countries have set various REN numbers.

Each device that can connect to the phone line has a REN. A device with a lower REN number has higher impedance, therefore requiring less current for the ringer to be sounded. Because it takes less current for a device with a lower REN, you can have more devices on the line. Devices include hand sets, fax machines, and answering machines.

If there are too many devices on the line and the sum of the RENs exceeds the set limit, the circuit will likely fail. It might just not ring or the phone company might temporarily disconnect the line to reduce the load.

Radio interference

Radio interference can be caused by bad wiring or from using cheap cabling. The electromagnetic interference (EMI) can be caused by electric motors, fluorescent lights, radio transmitters, lightning, and ham radio operations to name a few. The connection and the wiring can use shielding to protect the phone line from the noise RFI causes. This shows up as static on the line usually. While voice communication can usually cope with some noise, data communication cannot.

Crosstalk

The older four color wiring used up until the last few years suffered from crosstalk between wires in the cable. The older wiring has been replaced by Cat5 cabling in new installations. Crosstalk usually shows up as hearing all or part of another conversation on the line which you are using. Sometimes you can clearly make out what is being said; other times it presents as noise on the line.

By using twisted pair cabling, you can reduce or eliminate crosstalk. The twisting of the wires over each other cancels out the signals that are creating the crosstalk.

Crossed-lines are another way this might be referred to. This is usually when the conversation you are picking up is from wireless devices such as baby monitors, scanners, ham radios, and other cordless phones. Try switching devices to another frequency so that they do not interfere with the phone conversations.

Do it!

A-3: Identifying common POTS issues

Questions and answers

- 1 Explain the purpose of REN and what happens if you exceed the limits.

REN is a method of determining the load a device will place on a phone line. If you exceed the set limit, the circuit will likely fail. It might just not ring or the phone company might temporarily disconnect the line to reduce the load.

- 2 How does radio interference usually show up on the line?

It appears as static on the line.

- 3 What are some ways to eliminate or reduce crosstalk on the phone line?

Use Cat5 cabling, use cables with more twists, or switch interfering devices to another frequency.

Topic B: Voice over IP

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
3.1	<p>Differentiate and describe POTS vs. VoIP delivery. Identify and troubleshoot common issues.</p> <ul style="list-style-type: none"> • VoIP <ul style="list-style-type: none"> • Compatibility Issues • Whole House Distribution of VoIP • Performance and Quality of Services

Digital telephone communication systems

Explanation

Digital data transmission over telecommunications wires has several advantages over analog transmission, the two largest being that digital is much faster and much less error-prone. As it does on a network, digital data on a telephone line travels in packets. It follows the rules of established protocols, so that it can be controlled and sent to the correct address and interpreted when it arrives there. Voice data and other analog sounds are converted to digital form by sampling techniques similar to those used for digital sound recording. The coded audio signals are sent as digital data and decoded at the receiving end so that they can be “played” through a speaker as sound. Data sent by digital transmission, whether it is digital audio data, text data, or video data, travels far faster and with far fewer errors than it would as analog data.

As with analog signals, digital transmissions also weaken and pick up noise as they travel, but the amplification process used to strengthen digital signals is different from that used for analog. An analog amplifier must strengthen an existing signal including the data tones, variations, pauses, and noise that occur in it. The amplifier can’t change the data signal or any corruption that’s come into it. It can only amplify it and send it on. The distance that analog signals can travel is limited by the amount of noise that the signal picks up. Eventually the noise level becomes so high that the analog voice or data signal can no longer be understood.

Digital signals consist of only zeros and ones (binary numbers), which are very simple to read and to duplicate. A digital amplifier in a data transmission line is called a regenerator. Instead of amplifying the existing signal, the regenerator simply reads the signal and generates a duplicate signal of all the data in it but none of the noise. The clean duplicate signal is then sent on the line in place of the weakened one. Digital signals thus move more cleanly with less chance of error than analog signals, because they can be regenerated periodically without any noise being present in the regenerated signal.

Capacity in telecommunications is described as bandwidth. Analog transmission or POTS, whether voice or data, is narrowband, each line being limited to one voice channel or one data channel at a maximum speed of 56 Kbps. By contrast, a BRI ISDN line, though still narrow band in the digital data transmission scale, provides for two voice or data channels, each capable of carrying 64 Kbps and a third channel for control signals that can carry up to 16 Kbps. A T-1 line, which can be carried on two pairs of wires such as Cat5 or similar cable, can carry up to 1.54 Mbps of digital data.

This means that it can simultaneously transmit 24 data or voice conversations, each containing 64 Kbps of data. T-3 lines and other broadband technologies, transmitted over fiber optic cables or radio frequencies, can reach capacities ranging from 44.7 Mbps to 13.22 Gbps.

For most home telephone users, a Digital Subscriber Line (DSL) which provides digital data capacity from 128 Kbps to 7 Mbps or even more is adequate for both voice and network data requirements. Cost for a DSL line is usually less than for a T-1 connection, and DSL service is becoming available in ever wider areas, as telephone companies install additional lines. Where DSL service isn't available, users generally retain their analog telephone service and obtain digital data service through a cable company or a satellite hookup. Both cable and satellite services are more widely distributed than DSL, because neither is subject to the distance restrictions from a central telephone exchange that limit Digital Subscriber Lines.

There are several varieties of DSL, not all of which are available in some areas. Rural areas are unlikely to have DSL service available because of their distance from a central exchange. Distance of the user from the telephone company central office is a determining factor in the availability of all DSL lines. The following table shows various DSL line types and their distance limits from the central office (CO), typical speeds, and characteristics. Users should check carefully on the type and speed of service they receive when purchasing a DSL line.

Service	Upstream data rate	Downstream data rate	Distance limit	Voice?	Comments
Asymmetric DSL (ADSL)	1.76 Kbps 640 Kbps	1.54 Kbps 7.1 Mbps	18,000 ft. 12,000 ft.	Yes	Uses one wire pair
DSL Lite	384 Kbps	1 Mbps	18,000 ft.	Yes	Uses one wire pair
G.SHDSL	192 Kbps 2.3 Mbps 4.62 Mbps	192 Kbps 2.3 Mbps 4.62 Mbps	40,000 ft. 6,500 ft. 6,500 ft.	Yes	Uses one or two pairs
High-bit-rate DSL (HDSL)	1.54 Mbps	1.54 Mbps	12,000 ft.	No	Uses two wire pairs
HDSL2	1.54 Mbps	1.54 Mbps	12,000 ft.	No	Uses two wire pairs
Symmetric DSL (SDSL)	1.1 Mbps	1.1 Mbps	24,000 ft.	No	Uses one wire pair

Voice over IP (VoIP)

Data moving on a LAN or other network travels in packets that adhere mainly to the Internet Protocol (IP). Voice data packets can also travel on the same networks, provided they follow the same protocol.

Voice over IP (VoIP) systems must perform a number of tasks rapidly and flawlessly in order for voice telephone conversations to be sent over a network. When a voice call is made over IP, the sending system must encode the analog voice signal into digital form, compress the digital data to reduce its size, assemble the compressed data into packets with appropriate headers and trailers, and transmit the data onto the LAN.

At the receiving end, the data packets must be received on the LAN, reassembled into the order in which they were sent, decoded (decompressed and converted from digital to analog voice), and sent to a speaker (in a telephone or in a computer). All of this must be done as nearly as possible in real time because the telephone conversation is a two-way process and any appreciable delay in sending or receiving the transmissions results in periods of silence between every statement of the two speakers.

Data packets sent over a network don't need to arrive in sequence and can easily be sent again if a collision causes one to be lost. Voice data packets, however, are made up of parts of a real-time conversation and need to be reassembled at the receiving end in proper sequence and in real time. A lost packet or delayed transmission often causes the reconstructed voice to sound choppy or clipped and is difficult to understand. The biggest challenge for VoIP telephone transmission is to prevent the telephone conversations from being degraded significantly below the quality of analog voice transmissions.

To avoid significant degradation of VoIP transmissions, the network must have sufficient capacity so that only a small part of its data packets suffer collisions and must be sent again. The voice data packets must also be sufficiently compressed (uncompressed sound files are large) so that they can be sent and converted back into sound in real time, despite the delay caused by any lost packets. Providers of VoIP equipment are continually working on these two requirements in order to improve the quality of VoIP transmissions. New electronic chips that more efficiently compress audio and put it into packets for network transmission are being developed. Some of these new systems for VoIP also provide a means for voice data packets to have priority over other data packets so that the continuity of transmissions can be better maintained when traffic on the network is heavy.

Most home network users with IP-based phone systems still make the majority of their calls over the *public switched telephone network (PSTN)*. Intercom calls between nodes on the LAN are made over the network and long-distance calls can be made to a receiver node on another LAN that has appropriate software for decoding the data into voice. The installed number of such IP-telephone-equipped LAN nodes is growing because of its potentially low cost for long-distance phone service and its ability to make greater use of network infrastructure in place of new telephone wiring. The reliability of VoIP telephone systems isn't yet as high as PBX or key systems, which don't crash anywhere near as frequently as the typical computer system. Manufacturers are working on this problem, and the use of VoIP in business and in home LANs is increasing.

Remote access methods, standards, and protocols

VoIP systems can deliver telephone service to standard analog telephones, to PBX-connected or key system-connected multi-featured phones, or to soft phones built into a computer with software.

Soft phones are software programs that display phone features (hold button, caller ID, message waiting) on the computer screen and route the calls through a handset or an earphone and microphone wired to the computer. In addition to enabling VoIP phone capability with a minimum of new equipment (soft phone programs work with standard PC peripheral audio components), soft phones also can provide remote phone access. If the computer is a wireless laptop, then the soft phone system can go with it anywhere within the range of wireless reception. For the home user, this extends the telephone system to the full limits of the wireless hubs on the LAN without the need to install cordless phones or carry any additional equipment.

VoIP features

Compared to standard analog phone service, VoIP offers many additional features. Some features are also available on a regular phone line and some are possible only due to VoIP technology. One reason a lot of people choose VoIP over standard POTS service is that they offer unlimited long distance calling across the United States, often including Canada, and now sometimes additional locations around the world.

Call blocking, call waiting, call forwarding, three-way calls, and 411 services are some standard features available for both standard and VoIP services.

Many VoIP services provide an enhanced voicemail feature that lets you check your messages from your phone or another phone or from your PC or another PC. Some services offer virtual phone numbers that enable you to add additional phone numbers so that people calling you are calling a local number. You might also be able to use a different area code for this purpose as well. Check with the provider you plan to use for which features they offer. An extensive list of VoIP features can be found at www.whichvoip.com.

Some features of analog service are not readily available via VoIP, including fax capabilities. Faxing is available only via some VoIP companies. Fax machines require an analog phone line. Some VoIP services provide fax support, but most don't guarantee that all standard fax machines will work. Most suggest that instead you use email and sent the material as an attachment. This is sometimes referred to as an e-fax.

VoIP calls to 911 are routed to a Public Safety Answering Point (PSAP) rather than to an Emergency Response Center like regular phone calls are. PSAP will not receive information about your location like a call from a standard phone line would provide. You will need to tell them your location and phone number. Enhanced 911 (E911) provides the PSAP with the address on file for your phone number. Therefore, if you are not at that location when you place the 911 call, you will need to provide them with the location of the emergency.

Do it!

B-1: Defining VoIP features

Questions and answers

- 1 Compare amplification used with analog and digital signals.

An analog amplifier must strengthen an existing signal, including the data tones, variations, pauses, and noise that occur in it. The amplifier can't change the data signal or any corruption that's come into it. It can only amplify it and send it on. A digital amplifier in a data transmission line is called a regenerator. Instead of amplifying the existing signal, the regenerator simply reads the signal and generates a duplicate signal of all the data in it but none of the noise. The clean duplicate signal is then sent on the line in place of the weakened one.

- 2 List the bandwidth for each of these transmission types:

POTS

56 Kbps

BRI ISDN

Two voice/data channels at 64 Kbps and a control channel at 16 Kbps

T-1

1.54 Mbps

- 3 What is the result of lost packets or delayed transmission of packets in VoIP conversations?

It causes the reconstructed voice to sound choppy or clipped and it is difficult to understand.

- 4 Where are 911 calls routed to when using VoIP?

Public Safety Answering Point (PSAP)

- 5 What is the major issue about Enhanced 911 service?

The PSAP is provided with the address on file for your phone number rather than being able to tell where you are calling from as the analog phone system could. Therefore, if you are using a portable phone number and calling from a different location than the one on file, emergency crews might respond to the wrong location.

VoIP phones

Explanation



VoIP users have a wide array of phone choices. They can use existing analog or digital phones, they can use specially designed VoIP phones, or they can use software-based phones or phones connected to their computer.

Hard phones

A physical phone is often referred to as a hard phone. This is because it is a phone that does not require connection to a computer.

Analog telephone adapter (ATA) is used by some service providers to enable connection of an analog phone to a VoIP network. It has an RJ-11 jack to connect the phone and an RJ-45 jack to connect to the Ethernet network. This is also known as a VoIP gateway. Digital telephone adapters are available for digital telephones. ATA phones typically use SIP or IAX protocols

SIP is an IETF VoIP protocol that makes use of UDP and TCP over port 5060. An alternative protocol is *IAX*, which uses UDP port 4569. IAX works well in NAT (network address translation) network settings.

A VoIP phone contains an Ethernet interface to enable communication directly with the VoIP server, gateway, or another VoIP phone. No PC or software is needed. Cordless versions of VoIP hard phones contain the Ethernet interface in the base station.

VoIP DECT (digital enhanced cordless telecommunications) is a radio access technology. VoIP wireless phones contain a WiFi transceiver rather than an Ethernet jack. It doesn't require a PC or software, but does require access to a WiFi base station.

Soft phones



Soft phones require a PC running software that emulates the functions of a standard phone. The PC requires a sound card with either speakers or headphones and a microphone connected to the sound card. Alternatively, you can use a phone or headset that connects via the USB port on the computer. Some soft phones also support video, so if you want to take advantage of this feature, you will need a webcam connected to the PC as well.

Several of the popular instant messaging applications have added VoIP capabilities to their applications. Examples include MSN Messenger and Yahoo! Messenger. An extensive list of soft phones is available on the www.voip-info.org Web site.

Compatibility issues

VoIP services that plug directly into the network router should have no compatibility problems. You will need to make sure that the phone uses the same protocols as the service provider expects from the phone. Soft phones require that you download and install the version that is compatible with your operating system. In some cases, companies manufacture equipment to work with specific VoIP service providers and it will not work with other VoIP providers.

Skype

Skype is another option in the VoIP arena. This proprietary peer-to-peer network doesn't use SIP or IAX protocols. Instead, it uses its own proprietary protocol. It is available in a variety of formats, including:

- A software download for Windows, Mac, and Linux platforms
- Skype phones that can be used independent of a PC
- USB phones connected to a PC
- WiFi devices that work in any wireless network or public hotspot

From any of these types of phones, you can place free Skype to Skype calls. You can also place calls to other phones for a small fee. You can obtain a phone number so that you can receive calls from non-Skype phones as well. For a complete list of features and a description of which services are included for free, visit www.skype.com.

Whole house distribution

There are several methods for providing VoIP access throughout the house. If you are using a soft phone on a laptop or a VoIP DECT phone, you can carry it with you and have access anywhere within your WiFi area.

Another method is Powerline network. This is also known as PLC power line communication. It is a technology that delivers digital and broadband audio and video signals over AC power wiring or any other wire. For more information about this technology, refer to www.homeplug.org/en/products.

Do it!

B-2: Setting up and configuring VoIP access

Speakers or headphones and a microphone should be connected to the PCs.

If students do have an existing Skype account it would be distracting to have calls come in on it during class.

Here's how	Here's why
<p>1 If necessary, connect speakers or headphones to your computer's sound card</p> <p>If necessary, connect a microphone to your computer's sound card</p>	<p>You will set up Skype as an example of a VoIP service.</p> <p>You can connect a microphone or other device that includes a microphone. Some web cams include a microphone. The camera drivers need to be installed in order to use the camera's microphone. Some laptops have a microphone built into the case.</p>
<p>2 Access skype.com and download the software</p> <p>Install the Skype software</p>	<p>Follow the Setup Wizard steps, accepting all defaults, to complete the installation.</p>
<p>3 When prompted to create a Skype account, create one based on your name</p>	<p>If you already have a Skype account you will need to create a different one for the class. You can enter a fictitious email address if you don't plan on using this account in the future.</p>
<p>4 Click Skype Test Call</p> <p>Click the Call button</p> <p>Follow the spoken directions to record a message</p>	<p>To test your setup.</p> <p>This is the green button with an upright phone handset on it.</p> <p>To test your settings. You may need to adjust the speaker and microphone settings if you cannot hear the message you record.</p>
<p>5 In Skype, click Add Contact</p> <p>Add your partner's Skype name</p>	<p>Only one partner will complete this step.</p> <p>A message will appear on your partner's PC asking him or her to add you to the contact list.</p>
<p>6 Call your partner</p> <p>If your partner called you, click the green call button</p> <p>Click the red End Call button</p>	<p>One partner will place the call and the other will answer it.</p> <p>To answer the call.</p> <p>Either partner can click the red button to end the call.</p>

7 Close Skype

It is still running in the background. The icon in the system tray can be used to completely quit out of Skype.

In the System Tray, right-click the Skype icon and choose **Quit**

The Quit Skype? dialog box is displayed.

Click **Quit**

Quality of Service

Explanation



Quality of Service (QoS) is measured in several ways. It is a measure of how to guarantee that packets are not dropped or delayed due to network traffic.

To address the QoS issue, you need to look at:

- Packet loss
- Latency
- Jitter

Delays result in echoes the user can hear. Packet loss can result in the conversation breaking up or losing the conversation content completely. Strange noises on the line are the result of jitter, but buffers help with this problem.

Packet loss

Service Level Agreements (SLAs) for most VoIP service providers specify a packet loss of a maximum of 0.1 to 0.5%. A 1% packet loss results in errors that are easily detected by the users. In addition to packet loss that can occur on the provider's infrastructure backbone, the provider's and user's local networks can result in additional packet loss.

Latency

A roundtrip latency or delay of over 250 ms (milliseconds) is noticeable to the user. It is recommended that there be no more than 150 ms delay one-way. The entire path the call takes is included in the calculation. Therefore, this includes your network, your provider's network, as well as the Internet.

Jitter

The buffers used to compensate for network jitter add to latency. Timing delays on the network result in pauses in the conversation. The delay in the receipt of packets is referred to as jitter. A jitter buffers some of the voice data to help smooth out the delays. Too small a buffer results in discarded packets and poor call quality. A large buffer results in delays in which callers talk over one another. Setting a QoS policy on your network to give voice data a higher priority can help with delays.

*Do it!***B-3: Testing the quality of VoIP on your PC**

Here's how	Here's why
1 In a Web browser, open testyourvoip.com	You will use this Web site to test the quality of your VoIP network.
2 From the Call Destinations drop-down list, select the closest city	Testing will begin. A comparison to other communication methods is shown when the test finishes.
3 Click See Detailed Results Record the Round-trip Latency and Jitter results	
4 Click Test Again	
5 Choose a different city When the test finished, click See Detailed Results Compare the values with those recorded previously	

Topic C: Telephone systems

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
3.2	Describe and define fundamentals of telephone systems. <ul style="list-style-type: none"> • Multi-line • Paging • Intercom • Voice Messaging/Unified Messaging • Door Entry/Gate Entry • PBX • Key Systems • Telecommunication Services (for example, caller ID, voice mail, roll-over)

PBX systems

Explanation



If you need more phones, you might consider installing a *private branch exchange (PBX)* telephone system. A PBX is a private onsite switching system that routes calls within a single entity in the same manner as a central exchange routes calls on the public telephone system. The site for a PBX can be an entire organization, such as a business or educational institution, occupying one building or several. It can also be a small business occupying only a suite of offices or an individual home.

A PBX system controls telephone lines and switching from the *demarcation point* or demarc, the place where the incoming lines from the telephone company connect to the internal wiring of the home, to extensions and other devices throughout the house. Exhibit 4-3 shows the inside (user side only) of a demarc with three incoming telephone lines wired in it. The lower two lines are voice lines and are wired with old style, single-strand wire. The top line is a data line and is wired with new style wire.

Telephones are connected to the PBX rather than directly to outgoing telephone lines. The telephone lines leading out of the home to the demarc point are also connected to the PBX. Calls from one telephone to another in the home are connected through the PBX, and calls going out to the public telephone system are connected to an outside line through the PBX. Incoming calls on any line can be routed to any extension telephone within the home, again through the PBX.

D



Exhibit 4-4: An open three-line demarc box on a residence

Midsized businesses and other organizations find that PBX switching meets their needs more effectively and economically than Centrex. Calls going out of the PBX are carried on trunk lines to the central exchange, where they're routed on to their destination. Incoming calls travel on the same trunk lines. Most organizations with a PBX use a T-1 line for their trunk. A T-1 line can carry up to 24 voice or data lines simultaneously. Those 24 lines can be shared by 100 or more voice users, only a few of whom would be making calls simultaneously, and still provide data connections for the business as well.

PBXs are ground start systems. This means that, when a telephone receiver connected to the PBX is lifted to make a call, the PBX responds by sending a dial tone to the phone and also by requesting that an outside trunk line from the PBX to the central station be reserved or "seized" for the call. If the extension dials an access code (usually 9) for an outside line, it's connected to the seized trunk line, the caller hears another dial tone provided by the telephone company over the trunk line, and the call can be dialed. If the call is to an internal extension on the PBX system, it's routed directly to the called number and the seized outside line is released. Incoming calls are also sent over a grounded line seized by the central exchange when it receives the incoming call destined for the PBX.

Few homes have enough telephones or enough user demand to warrant installation of a PBX, even a small one. A large home having one or more offices with multiple lines and several additional home lines might want a PBX that could monitor outgoing calls from the business extensions in order to track expenses for tax purposes. Trunk-line service of less than a T-1 line, however, would hardly ever justify a home PBX, especially when another type of switching system is available for smaller users.

Exhibit 4-5 shows the back (connection panel) side of a home-size PBX system with a voicemail attachment on top of it. This system allows for three incoming trunk lines and up to eight residential extensions. It provides all standard PBX features including fax detection, which routes incoming fax calls to a designated extension.

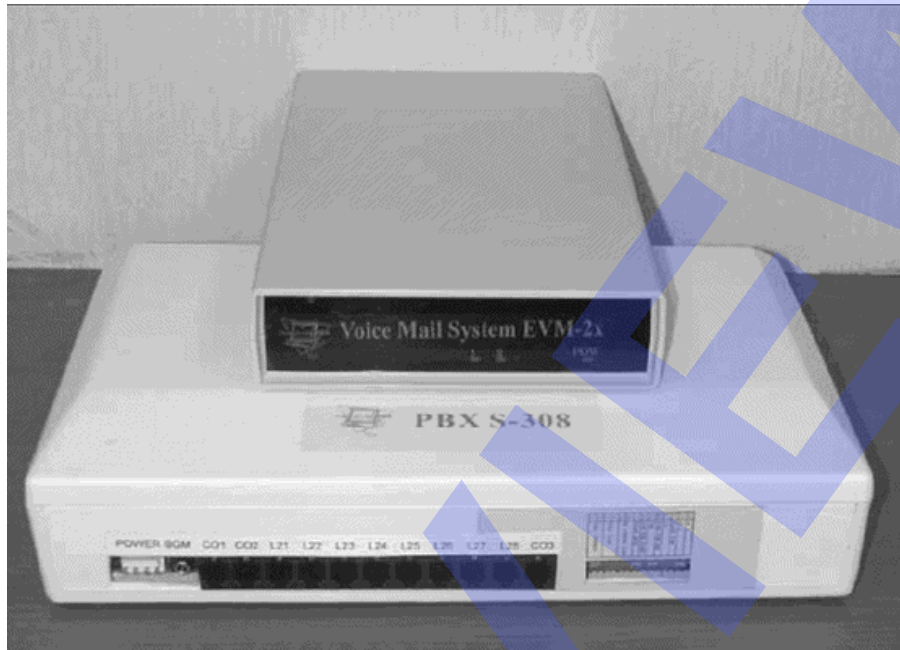


Exhibit 4-5: Small PBX and voicemail system suitable for home use

PC-based PBX

You can now install and configure a PBX system on a PC. One example is Asterisk, which runs on the Linux server platform. While this software is open source free software, you will still need to purchase PCI cards for the connection and appropriate phones to connect to either standard analog or digital phone services. This software is sponsored by Digium, and it is completely compatible with the Digium hardware. This is a VoIP based service that is highly customizable to meet various needs. More information about this technology is available at digium.com.

*Do it!***C-1: Connecting telephone extensions and lines to a PBX**

Here's how	Here's why
1 Connect the power supply cable to the PBX unit power port	You'll connect a telephone trunk line and two extension phones to a PBX so that calls can be made and received on the system.
Connect the PBX system power supply to an AC power outlet	
2 Connect a telephone extension to the L21 jack on the PBX	Use an RJ-11 patch cable.
3 Connect another telephone extension to the L24 jack	
4 Set the dip switches on the unit so that incoming calls from trunk link CO1 ring to extension L21	L21 will be the operator extension. Follow the instructions in the PBX for setting the dip switches.
5 Connect the CO1 jack on the PBX to a working telephone line jack	Use an RJ-11 patch cable.
6 Pick up an extension telephone receiver and listen for a dial tone	If you hear the dial tone, test the unit. If you don't hear the dial tone, check the dip switch settings and connections of the telephone extensions and line hookup.
7 Using extension 24 dial 0	To call the operator. Extension 21 should ring. If it doesn't, check the settings on the unit and change them so that Extension 21 is the operator extension, and then test again.

Key systems

Explanation



Key systems are designed for smaller organizations with fewer users than a midsize business. Key systems began when the old AT&T company began installing individual telephones connected to multiple lines. These phones had buttons or keys that could connect them to any one of several lines and a hold button that kept an in-use line connected while another line was used by the same telephone extension. Each line button had lights to show when a line was in use so that another extension user wouldn't push a button for a busy line (unless he or she wanted to listen in on that conversation).



On these early key systems, all the extensions could connect to all the lines simply by pushing a connect button to access the line. No access code for an outside line was required, because there was no PBX to request that an outside line be seized for a call. Key systems are loop-start systems rather than ground-start as a PBX is. This is the major difference between the two systems.

In a loop start system, when a telephone receiver is lifted to make a call, a dial tone is sent from the central office to show that a path is open for the call, but the line isn't seized until the call is actually placed. Likewise, an incoming call is sent to the destination number by any available path with no line being seized from the central station to the receiver in advance. This means that it's possible, though uncommon, that a user on a key system could pick up a telephone to make a call and find someone already on the line calling her or him, even though the telephone hadn't rung. The incoming call simply arrived over the available path slightly before the outgoing call could be placed. The loop path was filled first by the incoming call, which would have to end before the outgoing call could be completed.

Key systems with multiple loop start lines are well suited for small business users and homes with more than one line. All phones have access to all lines and can use any available line for outgoing or incoming calls. Key systems have an intercom button that allows them to make internal calls to other extensions without accessing an outside line. The internal call simply goes to the called extension over inside wires.

Intercoms

Key systems have intercom capability. An intercom link is simply an internal method of connecting two telephones without connecting either to an outside line. If there are four incoming lines with a key system, each phone has four line buttons so that it can connect directly to any of the incoming lines. It also has a fifth button for intercom calls. This button doesn't connect to an outside line, but to a switch panel that's also connected to each of the other intercom buttons on the other telephones in the home. As with the PBX system, each extension has a number, and any other extension can dial it directly, but only on the intercom line. If an outside line button is pressed for an intercom call, it can't connect, because those buttons connect the phone only to an outside line, not to the inside switch that links all extensions.

Intercom service is very useful in letting users in different areas of the home talk to one another without either person moving to the other's location. Some systems allow conference intercom calls (three or more participants) and many include a paging feature.

Paging allows one extension to call another and talk over a speaker on the called extension before the extension handset is picked up by anyone. One person looking for another can thus page him or her at various extensions around the house and yard (some paging features allow all extensions to be dialed for a page simultaneously) without having to shout his or her name or conduct a physical search.

Placing an extension at a door or gate entrance to the home can be useful. This allows the visitor to speak to you before you answer the door. This can be implemented using the paging feature or intercom feature of the phone system.

Hybrid systems

Newer key systems have most of the features of a PBX system and in fact may be hybrid systems that offer multiple-line buttons with the holding feature as well as the grounded trunk lines with a dialed outside access code used in PBX systems. These hybrid systems also offer many convenient features including:

- Hold buttons for keeping a line open
- Speed dial and redial buttons for rapid dialing of frequently called numbers
- Voice mail alert lights
- Caller identification screens
- Cordless telephone sets

These features and the multiple-line capacity of key systems and hybrids make them ideal for home use where multiple-line service is desired.

Both PBX systems and key systems carry voice calls over circuit-switched lines. This means that all the data in a call follows the same path on the network, and the line over which it travels is held open for that data for the duration of the call. Telephone systems have now converged with computer networks over which data is sent in packets that travel by different routes to the same destination. Manufacturers of PBX systems and key systems have now equipped their products with data transmitting capabilities using Internet Protocol. The result is Voice over Internet Protocol (VoIP) telephone service.

Do it!

C-2: Identifying telephone system features

Questions and answers

- 1 A PBX system is a private switching system that routes calls within a single entity. True or false?

True

- 2 What is a demarc in a PBX system?

The place where the incoming lines from the telephone company connect to the internal wiring of the home, to extensions, and to other devices throughout the house.

- 3 What type of line is usually used with a PBX system, and how many users can use the lines simultaneously?

T-1 line for their trunk. A T-1 line can carry up to 24 voice or data lines simultaneously. Those 24 lines can be shared by 100 or more voice users (only a few of whom would be making calls simultaneously) and still provide data connections for the business as well.

- 4 What's the major difference between key systems and PBX systems?

Key systems are loop start systems and PBX systems are ground start systems.

Voice messaging

Explanation

There is a variety of methods for callers to leave a message if the person they are calling is not available. Users can have standard answering machines, or they can sign up for a service with their phone provider that records messages on a central system accessible through a variety of methods.

In *voice messaging* systems, users are allowed to decide when and how they will access phone messages. It may also enable the user to specify how calls are routed. Voice messaging also lets users control the outgoing message for their voice mail. Users can treat voice messages as they would email messages, including using the ability to hear/view, store/keep, reply, forward, and delete messages.

Rollover

If you have a multi-line system one feature you might want to implement is call rollover. If the first line in your telecommunication system is in use, rather than sending the next call to voice mail, calls automatically rollover to a second line.

Unified messaging

People communicate over a wide variety of mediums including VoIP or PSTN phone, cell phone, email, and fax. *Unified messaging* integrates the various communications methods into a single interface to send and receive voice, email, and fax messages. It also sometimes includes instant message alerts if someone tries to send you a message.

The user can choose to be contacted immediately when a message arrives. They can also choose not to be alerted during specific times. This is sometimes referred to as “your time” communication.

Unified messaging enables users to hear email over the phone. Technology such as text-to-speech software enables this to happen. Alternatively, users might choose to access phone voice mails through email. This usually involves sending the message as a .WAV file attachment to a message sent to the user’s email inbox.

If the user is not at a PC, and while reviewing email messages on his or her cell phone finds that he or she would like a hard copy of an email that was sent to them, they might forward the message to a fax machine. Many users no longer use stand alone fax machines and choose to receive their faxes as email attachments.

*Do it!***C-3: Implementing a telephone system**

Here's how	Here's why
1 Open a search engine in a Web browser	You will search for a phone system that includes multiple lines, paging, intercom, voice mail, roll over and a unified messaging service compatible with it.
2 Search for a telephone system that supports multiple lines, paging, intercom, voice mail, and roll over	
3 Locate a unified message service compatible with the phone system you chose	
4 Determine the cost for the system and the unified messaging service	
5 Compare the features and costs with other students' results	

Unit summary: Telephony and VoIP

Topic A

In this topic, you described the characteristics of **analog telephone communication systems**. You learned that **POTS** is an analog voice telephone system that has been built as a worldwide network over a period of over 130 years. Its lines can also transmit data at a maximum speed of 56 Kbps. You also learned about the **wiring and jack standards** used for POTS connections. Finally, you identified **common POTS issues** including **REN**, **radio interference** and **crosstalk**.

Topic B

In this topic, you described the characteristics of **digital telephone communication systems**. You learned that digital telephone transmission of voice and data began in the 1960s and vastly expanded the data-handling capacity of POTS. Digital transmission of data, including voice, text, and video, can now be achieved at speeds ranging from 128 Kbps to 7 Mbps or more. You also learned about **VoIP** features. Next, you learned about VoIP phones which can be physical phones or software based phones. Finally, you examined **QoS** issues including **packet loss**, **latency**, and **jitter**.

Topic C

In this topic, you learned about local **telephone systems**. You learned that local **PBX** and **key systems** connect all local phones through a switchboard to trunk lines that go to the central exchange. Key systems connect multiple lines directly and provide intercom service. Finally, you learned about **voice messaging** and **unified messaging**.

Review questions

- POTS is an analog network of telephones and connecting lines. True or false?
True
- Data transmission over analog modems is limited to about _____ for receiving information and about _____ for sending information.
56,000 bps; 33,000 bps
- A PBX can connect _____ directly without the need of using any _____ line.
extensions; outside
- A PBX controls local telephone lines from the _____ to the end user extensions.
demarc point
- A soft phone is:
 - A a padded telephone
 - B a wireless telephone
 - C a computer-based telephone**
 - D a telephone with no speaker
- The standard plugs of terminating one- and two-line telephone connectors are _____ and _____.
RJ-11 and RJ-14

- 7 In the old-style telephone wire code, what colors are paired?
- A Blue/green and red/yellow
 - B green/red and black/yellow**
 - C white/blue and black/green
 - D yellow/green and black/white
- 8 If the first line in your telecommunication system is in use, rather than sending the next call to voice mail, which feature automatically directs the call to a second line?
- Rollover*
- 9 The feature that enables integration of various communications methods into a single interface to send and receive voice, email, and fax messages is known as _____.
- unified messaging*
- 10 In a _____, when a telephone receiver is lifted to make a call, a dial tone is sent from the central office to show that a path is open for the call, but the line isn't seized until the call is actually placed.
- loop start system*

Independent practice activity

In this activity, you will terminate both ends of a 10-foot Category 5 round or flat telephone cable with RJ-14 plugs.

- 1 Use a CatX cable stripper to strip the cable jacket 1 1/2 inches.
- 2 Place the stripped end of the cable in the jack and arrange the wires in the correct color code for an RJ-14 jack. Be sure the wires are pulled as far into the jack as the sleeving allows so that the excess stripped wire can be cut off when the wires are set.
- 3 Set the cable, connect it, and cut the wires using an RJ-14 punchdown tool.
- 4 Strip the other end of the cable jacket 1 1/2 inches.
- 5 Untwist and flatten the wire pairs in the correct color pattern for a two-line RJ-14 cable using a four-wire cable. If necessary, cut the stripped wires to a maximum 1/2-inch length.
- 6 Place the plug on the cable end with the flattened wires in the correct position. Be sure the wires are fully inserted into the plug.
- 7 Crimp the plug in place using an RJ-14 crimping tool.

PREVIEW

NOT FOR PRINTING OR INSTRUCTIONAL USE

Unit 5

Security and surveillance systems

Unit time: 240 minutes

Complete this unit, and you'll know how to:

- A** Describe basic security terminology.
- B** Apply installation procedures and methodologies
- C** Identify, configure, install, maintain, and troubleshoot security and surveillance cameras.
- D** Install and configure security panels.

Topic A: Security and surveillance system components

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
4.2	Describe basic security terminology and apply installation procedures and methodologies. <ul style="list-style-type: none"> Monitoring formats <ul style="list-style-type: none"> SIA and Contact ID 4/2 and 3/1 Define types of peripherals and accessories <ul style="list-style-type: none"> Motion sensors Glass break detectors Magnetic contacts Smoke fire (for example, smoke detection, heat detection) Environmental sensors (for example, carbon monoxide, gas, water, temperature) Vehicle detection Photo-electric beam devices Microwave beam devices Pressure sensors Sirens, strobes Security keypads Keyfobs Panic buttons

Security peripherals and accessories

Explanation

A security system is composed of a variety of sensors. These can be connected to a control panel or controlled from a software program. Depending on the sensors and what they are designed to detect, this will determine whether an alarm is sounded, a light turned on, or other events set in motion.

Motion sensors

Motion sensors or motion detectors are typically used to trigger an alarm in a security system. Some are used to turn lights (and sometimes music as well) on or off if a room is determined to be occupied or not. This is also referred to as an occupancy detector when used in this manner.

Most motion detectors use InfraRed (IR) detection, but some use ultrasonic pulses, which reflect off moving objects or use microwaves, bounce off objects. Sometimes two technologies are used in combination to reduce false alarms. This is useful for premises with pets since you can set the system to ignore smaller moving objects. Typically, wireless models ignore pets under 40 pounds and wired systems ignore pets under 80 pounds. This is often referred to as a pet-immune sensor.

The IR technology uses *Passive IR (PIR)* sensors. It is considered passive since the sensor doesn't emit any IR. All objects above the temperature of absolute zero emit infrared radiation. The PIR sensor contains a chip that connects to a circuit board to process the presence of an object in front of the sensor. Sensors contain either Fresnel lenses or mirrors to focus the radiation on the chip. Most sensors have a range of approximately 30 feet, although some larger ones can detect movement within 100 feet.

An example of a motion detector is shown in Exhibit 5-1.



Exhibit 5-1: A motion detector

Glass break detectors

A glass-break detector is a wired device that detects when a window is broken. The glass break detector is on the look-out for the high-frequency sound emitted by breaking glass. It is not the same as a window sensor, which detects a window being opened. These are often used in combination so that the alarm is triggered if either a window is smashed or if it is opened.



Magnetic contacts

Break switches are normally closed so that a current or magnetic force flows through them constantly. They're the type of sensor placed on window casings and doors. The switch is placed on the door or window casing, and the plate that completes the circuit in the switch is placed on the window or door. So long as the window or door remains closed, the switch plate keeps the circuit closed, and the sensor remains quiet. If the window or door is opened, the plate is pulled away from the switch, thus breaking the circuit. The sensor then sends a signal indicating that its circuit has been broken by the opening of the window or door.

Break sensors can be attached to any fixture where movement of one part opens the switch by separating the plate from it. Besides outside doors and windows, these sensors can protect cabinets containing valuables, rooms that shouldn't be entered, and objects that shouldn't be moved. An example of a magnetic contact sensor is shown in Exhibit 5-2.



Exhibit 5-2: A magnetic contact sensor

Smoke and fire detectors

Temperature sensors can be used to signal either high heat or cold. They measure the temperature of the air around them, and they have a normal range to which they don't react. If the air temperature rises above or falls below the normal range, the sensor signals the changed state. Some temperature sensors can record temperature changes degree by degree so that actions may be taken when certain levels are reached. Most, however, are simply switches that signal only when the temperature moves outside their normal ranges. Most are set to signal a temperature drop or a temperature rise but not both.

High-temperature sensors are used as fire alarms. They're usually mounted high in a room and signal a temperature change when air temperature at ceiling level reaches about 140 degrees. Since heat rises in a room, a fire burning at floor level will quickly raise the temperature at the ceiling to this critical level. Heat from a stove or other warming device won't get the air up to critical temperature unless these appliances are left on too long and become a fire danger. Temperature sensors don't react to smoke, only to heat, so they make good fire detectors in areas where some occasional smoke is common and smoke detectors can't be used.

Smoke detectors are sensors that constantly measure the purity of the surrounding air. Whenever the air becomes polluted with smoke particles, the smoke detector signals an alarm and usually an audible warning. Smoke detectors are the preferred means of fire detection, because they cost less than heat detectors and thus can be more economically placed throughout the home, but they do have some limitations. They're often set off falsely in homes where people smoke or where fireplaces or cooking smoke exist to any significant extent. When this happens frequently, the smoke detector is likely to be left off to stop the false alarms, and it thus becomes useless for its intended purpose. Smoke detectors don't react to heat, only to smoke, so a fire burning with relatively little smoke won't trigger them for a while.

Smoke detectors, like heat detectors, can be connected to a security system and trigger a call for the fire department when they go off, but this setup should be created only if false alarms are very rare. The fire detection system least vulnerable to false alarms may be one with smoke detectors in bedrooms, family rooms, and living rooms, and heat detectors in kitchens, furnace rooms, and wherever open fireplaces or barbecue grills are located.

The wiring for smoke and fire detectors needs to be special cable designed for this purpose that can withstand temperatures of up to 105 degrees Celsius. You should use 18-gauge red wiring with a red covering for fire alarm connections.

Environmental sensors

Low-temperature sensors are used mostly for freezing protection. Their normal range may go down to the mid 30s but, as the temperature drops to near freezing (32 degrees), they signal a temperature change. The security system may then be programmed to shut off outside water systems to prevent pipes from freezing. It may also activate deicing systems on driveways, roofs, and rain gutters. When the temperature rises again, these latter systems are shut down, although the lawn sprinkler system may remain off until a programmed length of normal temperature time has elapsed. Low-temperature sensors can also be useful in outbuildings where they can signal danger to animals or machinery when the temperature falls too low because of failed heaters, windows or doors left open, or some other mishap.

Water sensors are switches that react to the presence of water. Their normal state is dry. If they detect water, a circuit is completed and a signal sent to the central control. They are used to warn of water where it shouldn't be. The cause of such water can be leaking or broken pipes, seeping groundwater, excessive lawn watering, or any number of other causes. If the water is in the home's basement, it will likely cause damage. The water sensor can prevent that with a timely signal. A water sensor should be placed at the lowest point in the drainage area it's protecting. This allows the first water entering the area to trigger the sensor. The signal may start a pump working or merely send a warning alarm that something is amiss.



Water sensors are of two types, both of which can be very helpful in avoiding water damage in the home. The first is a flow meter placed in the main water line to the home. This device can monitor the flow of water in the home's pipes and sound a warning if the flow is excessive or if water is flowing at all in the hours when it shouldn't be. By checking the flow meter for the early morning hours, say from 2 until 4 a.m. when no water would normally be flowing in most homes, even fairly small leaks in bathroom fixtures can be found and corrected. A flow meter is very helpful in detecting water loss in leaking sprinkling systems as well.

The other type of water system sensor is simply a device that detects the presence of water where there shouldn't be any. Water sensors placed in dry areas or a basement can warn of a broken pipe or leaking appliance before serious damage is done. If the home is in an area where ground water is a problem, a basement sensor can alert the homeowner to incoming water as soon as it appears. If the problem is pervasive enough that the home has a sump pump, which is a self-starting pump installed in a pit below floor level to keep ground water out, then a water sensor is a necessity as a backup for the pump in case it fails mechanically or from lack of power.

Other environmental sensors that your system might include are:

- Carbon monoxide detector: detects the presence of carbon monoxide in the building and triggers an alarm.
- Gas leak detector: detects the presence of a natural gas leak and triggers an alarm.
- Rain detector: detects rain fall and turns off lawn sprinklers or triggers some other event such as opening an awning over the patio.
- Snow detector: detects the presence of snow on a surface such as a walkway, stairs, or driveway and activates heat coils to melt the snow.
- Weather sensors: sends information about the current weather conditions to the control panel or application which can then adjust settings in the house or on the property to accommodate weather conditions.

Vehicle detection

Using various types of sensors, you can detect a vehicle entering your property. This could be a pressure sensor that is activated when the vehicle drives over it. It could be a photo sensor that detects headlights shone at it. It could be a motion sensor that detects something passing it, although this could also be triggered by a person, so would not be the recommended method of detecting a vehicle. Various events could be triggered when a vehicle is detected ranging from turning on lights and opening the garage door to turning on music or TV news for a person arriving home from work.

Microwave beam devices

Microwave beams are often used to detect motion. A device sends out bursts of microwave radio beams and detects when the beam bounces back. When someone or something moves into the field covered by the microwave beam, the time it takes for the beam's reflection to return to the device or the amount of energy returned in the beam is detected. The device might be set to turn on lights, open a door, or trigger an alarm depending on what you have the device set up for.

This device type is often referred to as an active device since it sends a signal out and checks for changes in the return of the signal.

Pressure sensors

Pressure sensors can be used in several different applications. Pressure sensors are usually make switches.

Make switches are sensors in which the normal state is open and the changed state is closed. These are most often found as pressure pads that signal an alert if weight is placed on them forcing the switch closed and completing the circuit. Pressure pads can be found in driveways where they signal a car or other vehicle moving over them. They can also signal the approach of a person stepping on them. In either of these cases, the pressure pad might not signal any alarm because of the movement. It might simply trigger the opening of a gate or start a video camera to record the arrival or departure of a person. Note that a pressure pad doesn't tell direction of movement unless two are placed in line and successively tripped. Pressure pads are sometimes more useful as initiator devices than light beams or motion sensors, because their normal range can be set to exclude some weight but respond to anything over a set amount. Thus, the family dog or cat walking on the pad won't open the gate or door, but the weight of a person will. Likewise, the children can play on the driveway without opening the outer gate, because half the weight of a car is required to set it in motion.

In some cases, such as in historic homes where you don't want wires and sensors placed visibly on doors and windows, you can place pressure sensors near windows and doors to detect intruders. Their weight on the floorboards would activate the pressure sensor in this application.

Homes that have natural gas service for heating can monitor that service by means of a pilot light sensor connected to the security system. The pilot light monitor can be either a light sensor or a thermocouple. In gas heating systems without continuous pilot lights, a pressure sensor on the gas line can be used to confirm that gas is still available for use. Another useful sensor in the area of a gas furnace or water heater, as well as a gas dryer or stove, is a gas detector that can warn of a leak in the gas system. The vast majority of gas leaks result from an appliance inadvertently left on, or from a crack or burn-through in the gas-fired heating element of the appliance. A gas sensor placed in the room where these appliances are located can quickly alert the security system of a problem.

Sirens and strobes

Sirens are often activated when an intruder is detected. This serves to warn the homeowner of the breach and to hopefully deter the invader from remaining on the premises. However, for some of the population such as those in the deaf community, sirens are of little use. In those cases, a strobe can be activated instead of or in addition to the siren.



Security keypads

Security keypads are used to arm and disarm the security system. Most use a 3 or 4 digit number that you enter on the keypad. Some use more sophisticated technology such as fingerprint or retinal scan in place of or in addition to entering a security code.

Typically these are placed inside the main entrances to the home and one is often installed in the master bedroom so that the house can be set for protection after everyone has gone to bed.

Some systems enable you to enter one code for basic detection through windows and doors while you are still up and about moving through the house. Another code is then entered when retiring for the night so that any movement inside or outside the house triggers the alarm. An example of a security keypad is shown in Exhibit 5-3.



Exhibit 5-3: A security keypad

Keyfobs

While wall mounted keypads make it convenient to turn a security system on or off as you enter or exit a room, some users might like to have portable methods of arming or disarming the system. One option is a keyfob device. This also has the advantage of allowing arming and disarming the system from outside the premises so that you don't accidentally trigger an alarm on your way out. An example of a keyfob is shown in Exhibit 5-4.



Exhibit 5-4: A keyfob

Panic buttons

The wall keypad or the keyfob might have a button marked as the Panic button. This will immediately sound the alarm, and if so configured, call emergency personnel. Other panic buttons might be placed around the premises and indicated as such with labels and appropriate wording.

For the security keypad shown in Exhibit 5-3, press both E keys at the bottom of the keypad to sound the panic alarm. For the keyfob shown in Exhibit 5-4, press the two top buttons (Arm and Disarm) that are marked Panic.

Hand-held, wrist-watch-style, or pendant-style panic buttons might be used by those with limited mobility or who might have difficulty reaching a wall button. These are especially useful for elderly or disabled individuals.

Do it!

A-1: Identifying security peripherals and accessories

Here's how	Here's why
1 Locate a magnetic sensor switch	Your instructor will provide a variety of security peripherals and accessories for you to identify.
Locate a motion sensor	
Locate a device to arm and disarm the system	This could be a portable device such as a pendant or a keyfob or a wall mounted keypad.
2 Identify the method for invoking the panic feature on the keyfob or security keypad	
3 Describe two types of water sensors	<p><i>A flow meter in the main water line that is triggered by excessive flow or water flowing during hours when it shouldn't be.</i></p> <p><i>A water system sensor is a device that detects the presence of water where there shouldn't be any water.</i></p>
4 Pressure sensors are usually what type of switches? What does this mean?	<i>They usually make switches in which the normal state is open and the changed state is closed.</i>
5 What is the purpose of a siren or strobe?	<i>To alert the homeowner to the security breach and to hopefully deter the invader from remaining on the premises.</i>

If you have examples of the remainder of these devices, have students identify them as well.

Security monitoring formats

Explanation

There are several security monitoring formats in which messages to the security monitoring office are coded. They are SIA, Contact ID, 4/2 and 3/1 and include your account number and an alarm code.

SIA

SIA (Security Industry Association) is an international trade association for the security industry. There is also a monitoring format named SIA.

The SIA monitoring format uses codes that are sent as two-character event codes. Messages are variable length that can also include zone or user number, or an alphanumeric message.

The central office then has to translate these codes to numbers. The codes range from AA=1, AB=2 on up to ZZ=676. Not all codes in that range have been defined.

The code BA translates to the number 27, which is a burglar alarm. By default it dispatches police and notifies callout.

The code BC translates to 29 and is a burglar alarm cancel code to cancel a BA code that was sent fewer than two minutes before.

Contact ID

Another security monitoring format is *Contact ID*. It uses DTMF tones to send information. DTMF (dual-tone multi-frequency) is commonly known by the name Touch Tone. DTMF creates tones when a phone key is pressed. The tone generated is created from two tones: one from a high frequency and one from a low frequency. For example, pressing 1 creates a tone from a low frequency tone at 697 Hz and a high frequency tone at 1,209 Hz. The tone generated from pressing 0 is created from tones generated at 941 Hz and 1336 Hz.

Since it uses DTMF tones, using a standard phone line is the way most security systems were configured to contact the monitoring company or to dial out to whatever number you want the dialer to call when the system needs to signal an event. The newer VoIP systems do not generate DTMF tones, so an adapter is needed if you have such a system in order to generate the tones.

The Contact ID format was originally developed by Ademco, Group. It is now available for use by any company that wants to manufacture digital transmitters or receivers compatible with this format. This standard ensures compatibility between manufacturers who adhere to the standard. In this security format, the message sent contains:

- 4 character account number
- 1 character pin status: either alarm or restore
- 3 character alarm code
- 2 character dialer group, partition, or area number
- 3 character zone or user number

4/2 and 3/1

The way the message is sent from your security system to the central office needs to be configured in the format required by the equipment and the company servicing your account. In addition, you need to configure the dialer with the correct format. There are several formats which might be used.

The 3×1 format sends the account number as three digits followed by a one character alarm code. Only 15 discrete codes are available using the characters 0–9 and B–F. The 4×1 format is the same only it allows for a four-digit account number. Both of these must be configured with no parity in order for the message to be interpreted correctly at the central office.

Extended 3×1 format sends two separate messages. First a three digit account number and a one digit alarm code are sent. Next, the account number is sent again along with a one digit zone or user number.

The 4×2 format sends a four digit account number with an alarm code and zone number in a single message. Up to 225 unique codes can be sent using this format. The dialer can be set up with or without parity in this format.

Do it!

A-2: Identifying security monitoring formats

Here's how	Here's why
1 Access centralone.com/bulletins/BULL1033.TXT Examine the list of Event codes Identify the code for a gas alarm	You will examine features of various security monitoring formats This list contains SIA codes. GA 157 SPC
2 Access centralone.com/bulletins/BULL1032.TXT Examine the list of Contact ID codes Identify the code that indicates that smoke has been detected	This is a list of Contact ID codes. 111
3 How many unique codes are available in 3×1 and 4×2 formats?	3x1 provides for 15 unique codes; 4x1 provides for 225 unique codes.

Topic B: Security system installation

This topic covers the following CEA/CompTIA DHTI+ exam objectives.

#	Objective
4.1	Install, maintain, configure, and troubleshoot basic security systems and applications. <ul style="list-style-type: none">• Define monitored and notification methods<ul style="list-style-type: none">• Phone line• Cell phone• Radio frequency• IP-based
4.2	Describe basic security terminology and apply installation procedures and methodologies. <ul style="list-style-type: none">• Installation and configuration of security panel<ul style="list-style-type: none">• Zone types• Delays• Battery backup and power supply requirements• Describe security infrastructure types<ul style="list-style-type: none">• Wired<ul style="list-style-type: none">• 22/4-standard power devices• 22/2-magnetic contacts• 2- and 4-conductor FireWire-like keypads, sounders, power supplies, smoke and fire detectors• Power supervision relays• Polarity reversal relays• Line seizure• End of line resistors• Identify access control devices and protocols<ul style="list-style-type: none">• Devices<ul style="list-style-type: none">• Keypads• Card readers• Biometric readers• Proximity readers• Door strikes• Electronic deadbolts• Magnetic locks• Protocols<ul style="list-style-type: none">• Wiegand

Security infrastructure types

Explanation

Security systems use one of two types of infrastructure—the wired and wireless. A hardwired system has a wire connecting each part of the alarm system. The second is a wireless system that uses coded RF frequencies to control and track each part of the alarm system.

Wired infrastructures



In a wired infrastructure there is a 2- or 4-conductor wire connecting each of the detectors and keypads from the main alarm box. This is a very reliable and traditional system for security system infrastructures.

When wiring, if possible place each device into its own zone. It makes it easier to troubleshoot problems later.

Window sensors can be grouped together by room to create a zone. You can do this by running a wire from the control panel to the room, and then using a gang box to connect each window to this.

Smoke detectors should be installed in a daisy chain fashion, connecting one to the next and then to the control panel.

22/4 and 22/2

The 22/2 wire is a 2-conductor 22-gauge wire. It is used for door and window contacts, sirens, strobes, and power transformers. A shielded version can be used for remote temperature sensors.

The 22/4 wire is a 4-conductor 22-gauge wire. It is used for keypads, motion detectors, natural gas sensors, carbon monoxide sensors, and glass break detectors. This is the same wiring used for telephones.

Both types of wire are available in stranded or solid wire versions. A device that requires only two strands can use 4-wire cabling; you would just use two of the wires. Some devices such as sirens should use 18-gauge wire; you can meet this need by using 22/4 by using two strands of the wire for each of the connections on the siren.

Power supervision relays and end-of-line resistors

The 4-wire smoke detectors require the use of an end-of-line relay to supervise the voltage of the power line connecting the smoke detectors. This enables monitoring of all devices connected to the detector power line. The relay is placed at the end of the power circuit. Contacts in the relay are opened if there is a break in the detector power circuit, thus signaling the alarm to go off. It would also signal the alarm if there was a loss of power causing the power supervision relay to not be energized. For this reason, a battery backup is required on the circuit.

Polarity reversal relays

Polarity reversal relays can be used with 2- and 4-wire smoke detectors. This relay does not supervise the power line voltages. Instead, the interconnected control unit provides line supervision.

When a smoke detector goes into alarm mode, the relay reverses polarity of the input power. This enables all of the smoke detectors that are daisy chained together in a loop to sound their alarms. It functions the same way when used in a loop of heat detectors.

Notification methods

When an event occurs and triggers a response by the security system, you need to have a method of being notified of the event. You also would most likely want to have the system either directly dial emergency personnel or have it dial another person or service that could then check with you about whether emergency personnel should be contacted.

The alarm system often remotely communicates with a central monitoring station service. This is usually handled over a wireless RF communication network. Having parallel, redundant notification methods helps ensure that if one of the communication methods has been compromised, that another notification method is still available. For example, if by default, your system uses the phone line to place a call, the backup method could send an RF communication message instead.

Often, when a security breach occurs, the home occupants are not on site. You can have the security system notify you that the breach occurred. Notification methods include placing calls to either a cell phone or a regular phone. A pre-recorded message would alert you to the breach. A text-messaging capable cell phone could also receive a text message that was pre-programmed into the system to be sent out if an event triggered a response. An SMS message, a text message or an e-mail message could be sent using an IP-based messaging system connected to the security system. You can even have the message sent using all of those methods; this redundancy helps make sure that the event is made known to those who need to know.

Line seizure

Line seizure devices connect into an existing phone line and commandeer it in case of emergency. The device connects to alarm system dialer. The regular phone also connects to the device. The device disconnects any phone call in progress and sends its own generated busy tone to the phone. After a few seconds when a dial tone has been recovered by the emergency phone port, the emergency call is placed.

For VoIP lines, an adapter is needed to generate the dial tone. The dial tone is usually provided by the computer or VoIP adapter. Security systems still rely on the access of a dial tone to place calls.

Do it!

B-1: Examining security infrastructure types

Questions and answers

- 1 Identify where 22/4 and 22/2 wiring is used.

The 22/4 wire is used for keypads, motion detectors, and glass break detectors. This is the same wiring used for telephones. The 22/2 wire is used for door and window contacts. A shielded version can be used for remote temperature sensors.

- 2 Where are power supervision relays and end of line resistors used? Why?

In smoke detectors. The end-of-line-resistors detect a break in the power circuit and signal the alarm to sound. Power supervision monitors the line for power and sounds the alarm if power is lost.

- 3 What does a line seizure device do?

Enables you to use a single line for both regular phone calls and for use by the security system dialer. If the line is engaged, it will disconnect the call in progress and when a dial tone is reached, it will dial the emergency number.

- 4 List some of the notification methods that can be used in a security system.

Phone lines, cell phones for voice or text messages, RF, and text messages, emails, or other SMS messages.

Wireless security systems

Explanation

Wireless sensors don't require any wires either for signal transmission or for power to the unit. Transmission of data is handled by a transmitter, and both the sensor unit and the transmitter are battery powered. Good quality sensors and other wireless devices also monitor their batteries and signal when battery power is getting low. This feature enables the user to change the batteries in a timely manner without waiting until the sensor goes dead or by changing the batteries too soon and losing a large portion of battery life.

Power usage of wireless systems



Wireless sensors and their transmitters consume little power, and their batteries often last a year or more. However, the batteries used are typically 9- or 12-volt alkaline type and are three or four times the price of 1.5-volt C or D batteries. Action response devices such as audible alarms, emergency call-in devices, video cameras, utility controls, and intercom speakers can also be battery-powered. They are more usually wired, though, to an AC power outlet either directly or through a stepdown transformer. A *stepdown transformer* is a device that lowers AC voltage to the level required by the equipment. It's easier to power these devices with AC current, because they're nearly always located near a power outlet (appliance controls, lamp modules, and utility controls) or can be located near one (audible alarms and emergency call-in devices). Some response devices also require quite a bit of power to perform their functions, and battery power would be expensive to provide for these.

Some AC-powered devices do have battery backup power in case the AC connection is lost or the power in the home is cut off. These are primarily warning devices, such as alarms and emergency call-ins, which absolutely must function properly in life-and-death situations. Backup power for these devices is critical.

Signal transmission

Wireless sensors can transmit their signals to a security panel through walls and other obstructions within reasonable limits. The transmitters are low power, and their signals are degraded by distance. This means that their transmission range is limited to a few hundred feet. Heavy obstructions, such as concrete walls, metal structures, and other dense materials, can absorb some of the signal and further reduce its range.

For this reason, all sensors in a wireless security system should be tested after the sensors are mounted and the security panel is permanently positioned. Testing assures that the system is working under the actual range and obstruction conditions of the home. If either a sensor or the security panel is relocated, testing should be done again to be sure that all transmissions can still be received. If it's the security panel that's moved, all sensors should be retested.

Wireless video cameras are also available for home security systems, but most of the wireless transmitters on these units can work only across a direct *line of sight*. This allows the camera to be located in a good surveillance position without the need to be hardwired. It can then broadcast its images to a wireless receiver located in a position from which it can be wired to the monitor by standard video cable. Wireless video cameras can be battery-operated or connected to AC power through a transformer, if an outlet is available. To conserve battery power, wireless video cameras usually don't operate continuously, but only on a timed schedule or when signaled from the monitoring station to turn on.

Standards organizations and related technologies

Any discussion of home security systems based on either the HomePlug or *HomePNA* standards must of necessity be short. Despite the development expertise and power of the companies promoting these technologies through the alliances organized for that purpose, no viable home security systems have yet emerged operating on either standard. The same can be said of both the *HomeRF* and WiFi wireless standards: no company or consortium has introduced any significant home security products, despite the fact that home security systems are one of the two most sought-after applications of home technology integration. One WiFi manufacturer does offer a wireless video camera that can be set up as part of a home security system, but so far the company has made no discernable effort to market the camera in the home security context.

The wireless security systems manufactured by SkyLink, Honeywell, and others all operate on RF standards not related to any of the networking technologies. They also have no means of interfacing with any of the networking technologies, wired or wireless, except Ethernet. Not all security systems can interface with Ethernet, but we'll examine a couple that do and see how the network connection enhances the security function of both.

X10 security systems

Alone among the power-line technologies, X10 manufacturers have developed and marketed a wide array of security components and systems. These include not only sensors and security panels that operate on the traditional X10 technology of data transmission over AC power lines, but also a range of wireless devices that have greatly expanded the X10 system's capability and enabled it to interface with networks through an Ethernet port built into X10 components.

With power-line wired and wireless components, X10 security systems are actually hybrids that utilize both technologies to advantage in providing extensive, well-placed security protection and easily installed monitoring devices at convenient locations. Lighting control modules, the original automation devices for which the X10 technology was developed, can readily be incorporated as action response devices to any security alarm received. Appliance modules and other specialized devices can also be activated in response to a security signal or on a timed schedule as part of a monitoring routine.

X10 power-line system components

X10 security systems are hybrid wired and wireless systems. The wired portions of an X10 system utilize the home's AC wiring, and components are connected by being plugged into an AC outlet or wired into a wall switch. No new wiring needs to be installed for an X10 system. The security panel of the system requires AC power to function and so must also have a battery backup power source in case of power failure. The components that use the AC wiring for data transmission are battery-powered and signal the state of their batteries so that no backup power is required. The data transmission of an X10 system isn't affected by AC current flow in the wiring or its absence: the system's sensors function with or without AC power.

The wireless components of X10 systems are also battery-powered and can be installed without regard to a power source. Some broadcast directly to the system's security panel, but others (notably the video surveillance cameras) may broadcast only on a direct line of sight to a receiver some distance away. The receiver must then be wired into the security system in order for the broadcast signal to complete its journey.

For video cameras, this means wiring the receiver with a video cable to a monitor or switch panel. For sensors that broadcast to a remote receiver, the receiver can be connected to the AC wiring through an outlet, and the signal received from the wireless unit is relayed from the wireless receiver over the AC power line to the security panel.

There are many X10 security system packages available on the market. Most include only the basic components that are required in almost every home security system. These can be augmented with an enormous array of additional devices to customize and complete each individual system. Exhibit 5-5 shows a typical basic system offered by SmartHome, a large supplier of X10 systems. The system includes the following items:

- One PRO2000™ security control panel (including alarm siren and call-in function)
- One motion sensor
- One handheld remote
- One keychain remote
- One X10 lamp module (to control lighting)
- Two window/door sensors



Exhibit 5-5: Basic X10 security system components

To install the X10 security system, the security panel is connected to the AC power through an outlet (the unit's AC cord also connects it for data transmission). The remote AC units (light modules and some sensors) are similarly connected by being plugged into wall outlets in appropriate locations. The wireless components function like any wireless system and are installed where needed. All sensors and lamp modules must be set with a house code and unit number, so that their transmissions can be identified by the control panel. These numbers are set with selector wheels mounted on the units or by programming buttons located under the battery covers.

X10 systems have many control options available, including touch screens, telephone links, remote wireless controls, and computer links with software so that a system can be controlled and monitored on a PC.

Do it!

B-2: Discussing wireless security system installation

Questions and answers

- 1 How are wireless security systems powered?

Wireless sensors and transmitters are typically powered by 9- or 12-volt batteries. Action response devices are typically AC-powered but might be battery-powered or have a battery backup.

- 2 What factors affect wireless signal transmission?

Distance and heavy obstruction, such as concrete walls, metal structures, and other dense materials

- 3 How is X10 technology used for home security?

Lighting control modules, the original automation devices for which the X10 technology was developed, can readily be incorporated as action response devices to any security alarm received. Appliance modules and other specialized devices can also be activated in response to a security signal or on a timed schedule as part of a monitoring routine.

Explanation**Access control devices**

Access control devices are devices that monitor an entry point. Entry may be restricted completely or electronically keyed to a keypad or other device that allows only specific persons to enter without setting the alarm off.

Keypads

Keypads are a common access control device. Users enter a code to open the door. Some can be set with individual codes for each user. Others use a common code for all users.

Keypads should be located near the doors they serve but also in plain sight, so anyone using them will be visible to passersby. Wireless keypads can be mounted directly on the door above the doorknob. Hardwired units need to be placed on a wall with access to power. Most wired keypads and some wireless ones operate on either 9–16 volts or 20–26 volts. The power can usually be either AC or DC and is stepped down (reduced) from the 120-volt current in the home's electrical system by a transformer.

Some wireless keypads are battery-operated, as are the locks they control. These units require a battery change at least annually, and more frequently if use is heavy or if the unit is located where it's subjected to a lot of heating from sunlight. (Heat increases the chemical reaction of batteries, depleting their power more rapidly.)

Battery-operated keypads are usually 6–9 volt units, while the locks often use 12 or more volts. The expense of battery replacement may eventually outweigh the convenience of wireless installation for these keypads and locks. Nonetheless, they offer security protection as good as the hardwired units for considerably less initial expense. Exhibit 5-6 shows on the left a battery-powered keypad lock, which is self-contained and functions somewhat like a combination padlock or safe. On the right is a typical front door area keypad location.



Exhibit 5-6: A self-contained keypad lock (left) and a wall-mounted keypad for a lock

Keypads and other access devices, such as swipe slots for magnetic keys and identifier pads for fingerprint impressions, should be located high enough from the ground that small children won't be tempted to play with them but low enough so that the home's occupants can easily access them for input. Between four and five feet from ground level is the usual height for these devices, and this height may mean that they need some protection from sun and weather if the door is in an unsheltered place. This may consist of a protective cover or similar shield. Such covers should open to the side, not to the top, so that they remain open without being held, and only one hand is required to access the keypad or identifier unit inside.

Card readers

Card readers are a common access method for businesses. Employee badges are also the card swiped through the reader to open doors. All cards might work on common entrance doors while only authorized user's cards can be used to enter a lab area or a network server room.

There are a variety of technologies used for cards used in card readers. These include (from lowest to highest security):

- Barcode
- Magnetic stripe
- Wiegand
- Proximity
- Proximity used in conjunction with a keypad
- Biometric

Exhibit 5-7 shows a standard double-cut mechanical key on the left, a metal Marlock key with a numeric password encoded on it in the center, and a plastic magnetic-stripe key on the right. Both of the encoded keys work electronically. They have a numeric combination recorded on them that can be unique to every key, and it's read by the security system when the key is inserted into the lock or passed through a reader. If the numeric code is recognized, the lock opens.



Exhibit 5-7: A mechanical key (left) and two encoded electronic keys

Electronic key cards have the additional security advantages of being very difficult to duplicate and being recordable every time they're used. Being difficult to duplicate prevents a would-be intruder from copying the key and also prevents the rightful owner from inadvertently or deliberately giving away the password on it. Neither the owner nor anyone else can read the password or see it entered, so it remains secure no matter how the key is used. If the key is lost or stolen, the password on it can simply be blocked on the security system. No other keys are affected, and no change of locks or other devices is required to maintain security.

Recording the use of electronic keys allows the homeowner to monitor who's using them and when. Each time a key is inserted in a home lock, the security system records its password and the time it was used. All entries into the home are thus recorded and, if any security problem later develops, the users of the keys can be traced through the file in the security system.

Biometric readers

Biometric identification systems are presently not used much in home security systems but may become more common in the future. They simply take the password concept to another level by identifying authorized persons according to something unique in their physical makeup.

Fingerprint readers have also been used at amusement parks to verify that the person presenting the season pass at the gate is the authorized user of the pass.

Biometric identifiers include a fingerprint (usually a single thumb print impressed on a sensitive pad and scanned into the security system), a retinal scan, or a photographic image of a person measured for uniquely distinguishing features by the security system. An example of a fingerprint scanner is shown in Exhibit 5-8. All these identifiers are unique to every individual and so offer an absolutely secure means of identifying the person who's authorized to enter a secured area. Since these identifiers form part of the individual's body, they can't be loaned out, duplicated, or stolen.



Exhibit 5-8: A fingerprint scanner

Proximity readers

Proximity readers enable reading a key fob or card held 4 to 24 inches from the reader. This is an RFID device in which information about the user of the fob or card is embedded in the card or fob. This is a secure access method; however, it doesn't verify that the holder is the person authorized to use the fob or card. For this reason, it is often used with another access control method such as entering a PIN number that is known only to the authorized user.

Some readers are programmed using a keypad on the reader. Some are programmed via computer. Still others require a separate programming device or special keys to program them.

A record of who accessed the reader and when is maintained by the reader. This creates an audit trail that can be used as needed. The information can be downloaded to a computer.

Door strikes

A *door strike* is installed on the door frame across from the door latch. An electronically controlled door strike plate allows the door to be unlocked by an electronic signal from the alarm system via a central control, card reader, biometric reader or keypad. Using an electric door strike requires that the door handle be unlocked from the inside. These are usually 12V direct current devices with low power consumption.

Electric door strikes are available in fail safe and fail secure designs. A fail safe lock only remains locked if it receives power. If the home loses power, the door will be unlocked. This is good and bad: good in that people can leave; bad in that it remains unlocked after people leave. A fail secure lock remains locked even if the lock fails to receive power, such as doing a power outage.

Electronic deadbolts

An *electronic deadbolt* is a deadbolt lock that can be opened or closed via an electronic signal from the alarm system. The signal might originate via a central control or card reader, biometric reader or keypad. Some models are available that also can be operated by key in the event that power goes out, making them fail secure devices since they remain locked when the power goes out. In some models the bolt is only projected when the power is on, making them a fail safe device rather than a fail secure device.

A deadbolt is mounted in the door and the bolt extends into the door frame. A plunger lock is installed in the door frame and the bolt extends into the door. The plunger type of lock is most often used on full-swing doors.

Magnetic locks

A magnetic lock is also known as an electromagnetic lock since it uses an electromagnet to keep a door closed. Most often these locks are installed at the top of a door. These are often used on glass doors. Typically electromagnetic locks can hold a door closed with over 1000 pounds of force. As with the other lock types this can be opened or closed via an electronic signal from the alarm system. These locks are available in fail secure and fail safe configurations.

Access control protocols

A *protocol* is a set of rules and standards that define a communication standard. By defining a standard, various companies can write programs and create devices that will interoperate as long as they all follow the protocol as it is defined.

Wiegand access control protocol

The *Wiegand protocol* is an access control protocol based on principles discovered by John Wiegand. Embedded within a card are coils of ferromagnetic wire. Using the wire's magnetic field, polarity is changed and pulses are generated. The pulses are known as the Wiegand Pulse or Wiegand Effect.

This protocol has been in use for many years. Most proximity, biometric and wireless readers are able to make use of the Wiegand protocol. The Wiegand protocol provides a standard method of communication between the readers and the controllers. This is a relatively low security protocol. For example, there is no way to prevent the duplication of security cards.

The sensor and card trigger the processor to open the door. The wire within the card can be encoded using 24-bit encryption to create over 65,500 unique codes. The protocol defines a standard packet as 26-bits long. In addition to the 24-bit encrypted code, there is an even parity start bit at the head of the packet and an odd parity stop bit at the end. The cards can be further programmed to work with specific systems. The first 8 bits of the packet identify the facility. The remaining 16 bits identify the user.

A 30 bit version of the protocol has a 28-bit encryption size. There is also a 34 bit version of the protocol. It contains an additional 8 bits to define the user code, thus enabling more users to be uniquely identified.

Other protocols

More secure protocols have been defined. One reason for this is to prevent duplication of user security cards. Examples of more secure formats include the XSF and KSF protocols. The XSF is a 39 bit protocol. The KSF is a 34 bit protocol. While these are more secure, they work with fewer security card readers. Examples of proximity readers they do work with are IO-Prox readers and Shadow Prox readers.

Do it!

B-3: Identifying access control devices and protocols

Questions and answers

1 Which of these are true of keypads? (Choose all that apply)

- A** Often include electrically operated door locks.
- B** Can be opened using remote transmitters.
- C** Always have a key lock mechanism.
- D** Can be deactivated so that even entering the correct code doesn't unlock the door.

2 For a password-protected lock, only one password can be assigned. True or false?

False

3 What enhancements have increased the security of keys?

Keys with passwords, electronic keys connected to security systems, time coding so they work only at specific times

4 What are some of the biometric features that can be used for identification?

Fingerprint, a retinal scan, or a photographic image of a person

5 Which access device would you recommend to a client who wants to minimize cost but have the most secure access device possible?

Answers will vary, but keypads and electronic keys are probably the most cost effective.

6 Explain the structure of the Wiegand protocol.

It starts with an even parity bit. Then there are 24, 28, or 32 bits of encrypted information. The first 8 bits of the encrypted portion identify the facility and the remainder identifies the user. It ends with an odd parity bit.

Security panels

Explanation

The *security panel* is where all of the wires for a wired security system come together. If possible, place the security panel near the phone line access point to the house. This will enable you to easily connect the security system to the phone line. If you have a central wiring closet for all of the other wiring needs for the house, the security panel will also reside in that closet.

Zone types

Each circuit connected to the security control panel is a separate *zone*. If you connect multiple control devices to a single circuit, the security system will not be able to tell which device tripped the alarm. For example, if you have a door alarm and a PIR device on the same circuit, you won't know whether someone opening the door caused the alarm to sound or if it was movement in front of the PIR. When multiple devices share the same circuit, this is referred to as a subzone.

Most panels have between 6 and 48 zones. An 8 zone system is adequate for a house with 3 entry doors, and monitoring of access to 4 rooms provided you don't care which of the two windows in the Living Room that the burglar came through. The eighth zone is usually reserved for panic alarms.

Wireless security systems use the zone concept as well even though there are no wires to define each zone. Each device has a port on the security panel and can be identified through this port as a particular zone.

Delays

The main programming of a security panel is for the outside and inside arming of the security system. Having a delay enables you to exit the building without setting off the alarm on your way out the door, provided you exit within the time set for the delay.

Outside arming activates all security sensors to function while the home is unoccupied. The outside armed state is usually set by entering a command code on a keypad near the home's entrance when the occupants leave. The code can also be entered on the security panel itself. In either case, after entry of the code, a delay follows during which the occupants leave the home and secure the entrances. When the delay expires, the security system activates all sensors inside and outside the home and sounds a chirp or bell to confirm that it's functioning.

When the home's occupants return and open a door to enter the home, another delay is activated during which the security system must be disarmed, so that it won't interpret the homeowner's return as an intrusion. Typically, a 30-second delay is sufficient to disarm the system. During the delay, most systems sound an intermittent beep to remind the entering person that an alarm will be triggered if the system isn't disarmed. Exit codes, exit delays, and entrance delays can all be varied to suit the needs of the owner.

Inside arming activates perimeter devices in the security system and may activate some interior devices but usually not all. Inside armed is the normal status for the security system at night while the family is asleep. All window and door sensors and any sensors and detectors in the yard are active. Some inside motion detectors, such as those that guard doors, might also be activated, but motion sensors covering broad areas of the home's interior are left inactive. These provide additional protection when the house is empty (outside armed). However, they create too high a risk of false alarms to use with inside arming, because anyone moving in the home at night could set them off.

Inside arming is done from the security panel and involves no delays, when either arming or disarming the system, because the home's occupants can still move about freely with the security system functioning in this mode. Many systems allow inside arming to be set by a timer so that it activates every night at, for example, midnight and disarms automatically each morning at 6 a.m. Timing the system eliminates forgetting to arm it (or disarm it), and the schedule can be overridden manually with different settings when necessary.

Battery backup and power supply requirements

Many home security systems have backup battery power, which can be used in case of power failure, or some type of failsafe system that warns if power is low or sends an emergency signal in the event of power failure. This backup power method is sufficient for most systems, but if the home network has an *uninterruptible power supply (UPS)* for use in maintaining all or part of the LAN's operational ability during a power failure, this power backup can easily be configured to include the home security system. Security panels don't require a lot of power and so won't put a heavy drain on a UPS designed to supply and protect the network.

A 12- or 24-volt security panel powered by an AC adaptor can simply be plugged into one of the UPS outlets, and the unit is supplied through the UPS. Wired sensors that are powered from the security panel are also powered by the UPS through the adaptor hookup. Wireless devices that are battery-powered can't be connected to a UPS, but they also aren't affected by a power failure and shouldn't need backup power. Their low-battery warnings should always be heeded so that they don't lose battery power in an emergency situation.

Home UPS systems are battery-powered and have limited operating times under load. They're not designed to keep large systems running, only to give enough time for orderly shutdown so that no data is lost. The home security system won't tax a UPS nearly as much as the LAN will, but when other devices deplete the UPS batteries, the security system shuts down as well. In the event of power failure, the operating limits of the UPS should be noted and the homeowner should be aware that the security system ceases functioning when the battery power runs low.

Whole-house generators are now within the price range of many home owners. These are intended to provide longer term power than the typical UPS system described above. These are connected to a natural gas line or an LP tank as their power source to power the batteries contained within the generator.

Do it!

B-4: Installing and configuring a security panel

Here's how	Here's why
1 Connect the X10 Supervised Security System to a wall outlet	
2 Set the House Code to a unique value	Each student needs a unique House Code.

Topic C: Security and surveillance cameras

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
4.3	<p>Identify, configure, install, maintain, and troubleshoot security and surveillance cameras.</p> <ul style="list-style-type: none"> Camera Types <ul style="list-style-type: none"> IP Analog Hybrid Camera Specifications <ul style="list-style-type: none"> Lens Type • B&W vs. Color Lux Rating • IR Illumination Resolution • Power Consumption Camera Applications <ul style="list-style-type: none"> Indoor/Outdoor • Surveillance (for example, door cams, nanny cams) Day/Night • Recording (for example, DVR, Triggers – internal vs. external detection) Fixed vs. Animated • Sequencing vs. Multiplexing

Camera types

Explanation



There are two basic types of cameras in use today. One is the digital camera. The other is the analog camera. They are both capable of high quality surveillance, provided they are properly installed.

IP

IP cameras are digital cameras that can be connected directly to the network rather than to a computer. Many contain an embedded operating system and even an embedded Web server. Since the camera has an IP address, it can be accessed via a Web browser.

Typically IP cameras are low resolution images sized between 150×120 and 640×480 pixels. However, some send high resolution video streams.

Some IP cameras are connected using Power over Ethernet (PoE). This provides both power for the device and a data path on a single Cat5 Ethernet cable. A single network cable can support over 220 cameras.

Analog

Analog cameras output an analog signal. Analog cameras require a separate coax cable for each camera. The cable can connect to a video recording device, to a monitor, or using a splitter, to both. The images cannot be accessed from remote locations.

A number of factors can cause degradation of analog images. One is *attenuation*. When the signal must travel over a long distance, the signal quality of the image deteriorates over distance. Another potential problem is interference from radio, fluorescent lights, electrometrical motors, and other electronic devices.

The wireless video camera shown in Exhibit 5-9 is an example of an analog camera. This is an indoor/outdoor model that is weather resistant.



Exhibit 5-9: A wireless video surveillance camera (right) and its receiver

Hybrid

By connecting analog cameras to a video network you can digitize analog input. The data can then be accessed over the IP network from remote locations.

Some cameras are capable of connecting to digital or analog devices. If using the camera in IP mode, set an IP address and connect it to an Ethernet connection so that you can view and control the camera using a PC. In analog mode, the camera can be connected using coax cables to connect to a traditional monitoring system.

Camera specifications

There are several factors to consider when comparing cameras. How the camera will be used will affect the specifications you need to look at.

Lens type

As with other cameras, surveillance cameras offer a wide variety of lenses. The less expensive models usually contain a fixed focal length lens. The field of vision narrows as you bring the fixed focus camera closer. For example, a 25mm fixed length lens at 100 feet can capture a span of about 18 feet wide and if you bring the camera closer, say to 25 feet, you can only capture a span of about 4 feet wide.

For those cameras used outdoors or in variable lighting conditions, a lens with an automatically adjustable iris for adjusting to the current lighting condition is invaluable.

Some other lenses you might encounter include:

- Fixed-dome: Allows the camera to point in various directions without observers knowing where it points to.
- Fish eye: A wide angle lens that enables you to see an entire room at one time, but the image is somewhat distorted.
- Wide angle: Good for confined areas where you want to see as much as possible of the area.
- Telephoto: Good for close-up detailed images, but you lose the range of the wide angle.
- Night lenses: Improve sensitivity of components for low light conditions.

Lux rating

Lux is a measurement of how much light falls on an object. It is also known as a lumen and is equivalent to 1/10th of a foot-candle. It is measured as the amount of light falling on a one square meter area from a single candle one meter away. A measurement of 5 lux would indicate 5 candles at a one meter distance.

The *lux rating* describes how much light is required for an acceptable image to be captured by the camera. This is a subjective measure since what is acceptable to one person might not be acceptable to another person. Therefore, just because two companies say their cameras operate at 0.5 lux, that doesn't necessarily mean that they are capable of the same level of quality in low light conditions.

Some cameras can operate at 0 lux. Light colored and reflective surfaces are easier to capture in low light conditions than are dark colored non-reflective surfaces. So, these low light cameras still would have more difficulty capturing dark images and light images.

Resolution

The *resolution* of the camera refers to the level of detail that can be attained with the camera. Surveillance camera resolution is usually measured in TV Lines (TVL) which are the number of horizontal lines on the screen. An average resolution is between 350 and 400 TVL. High resolution screens are in the 480 to 500 TVL range.

Some cameras are advertised using pixel measurements, but this is not as accurate of a measure as TVL is for surveillance cameras. When referring to image resolution by pixel, you need to look at the image dimensions. For example, 720×480 pixels is the NTSC digital video standard.

B&W vs. Color

Black and white cameras used to be the only affordable option in surveillance cameras. Prices have dropped now so that color is quite affordable and some companies no longer even produce black and white cameras.

Black and white cameras are often able to capture better images in low light situations. However, if you can tell the police that the intruder was wearing a green shirt under a blue coat that will be more useful than being able to tell them he was wearing dark clothing.

Some cameras have the ability to switch between color and black and white images. When the lighting conditions are too low to capture acceptable color images, the camera automatically switches to black and white mode.

IR illumination

In very low light conditions *IR illumination* is useful. This type of illumination lets you illuminate an area where you do not want visible lighting. The visible light spectrum is in the 400 to 750 nanometer (nm) range. IR light in the 800 to 1200 nm range is close to this visible spectrum. The area being captured by the camera can be captured using this IR illumination. It is also the method often used when filming to keep the scene dark.

Higher quality IR cameras will have more LEDs which will illuminate the area over a greater distance. It will give a superior image over those with fewer LEDs out to about 50 to 60 feet.

Power consumption

There are two types of digital surveillance camera image sensors: CCD and CMOS. The processing power required by CCD is up to 100 times greater than that for CMOS cameras.

Charged coupled device (CCD) is able to create high quality images. This is an integrated circuit used in cameras for the image sensor function of the camera. It contains many light sensitive capacitors which are coupled together, thus giving this its name. These are found in high-end digital cameras.

The other is CMOS-based and produces lower quality images. This image sensor uses a CMOS integrated circuit in the camera. It is much less expensive than a CCD based camera.

Do it!

C-1: Discussing camera types and specifications

Questions and answers

- 1 Compare analog, IP, and hybrid cameras.

Analog cameras connect to traditional monitoring devices via a coax cable and cannot be viewed from remote locations. IP cameras are digital cameras that connect to the Ethernet network and are assigned an IP address; they can be viewed remotely. Hybrid cameras are capable of being connected via coax and used in analog mode or connected to the Ethernet network with an IP address.

- 2 Identify advantages of using fixed-dome, fish eye, wide angle, telephoto, and night lenses.

- *Fixed-dome: Allows the camera to point in various directions without observers knowing where it points to.*
- *Fish eye: A wide angle lens that enables you to see an entire room at one time, but the image is somewhat distorted.*
- *Wide angle: Good for confined areas where you want to see as much as possible of the area.*
- *Telephoto: Good for close-up detailed images, but you lose the range of the wide angle.*
- *Night lenses: Improve sensitivity of components for low light conditions.*

- 3 What does the lux rating indicate?

How much light is required for an acceptable image to be captured

- 4 Why would you want a camera to capture images in black and white rather than color?

Most cameras have trouble capturing acceptable color images in very low light conditions such as a night. Being able to switch to black and white mode enables the same camera to function at night.

- 5 About how far will IR illumination reach?

About 50 to 60 feet

- 6 Which type of image sensor creates a higher quality image? Which uses more power?

CCD

Camera applications

Explanation

The reasons for installing cameras and the locations in which they are installed will vary widely depending on the users' needs. Some people are only on the lookout for intruders. Others are monitoring children's activities or the area around a swimming pool or outdoor trampoline. Still others simply want to see who is at the door before determining whether to answer the door or not.

The cameras that you choose to install will vary based on the locations and their uses. You might want to record what the camera sees and keep it for a period of time, or you may not need to keep a record of what happens, and just need it for real time applications.

Video cameras located at strategic points around the exterior of a home and at the entrances provide a means of visually checking the area in view of the camera. This placement allows the homeowner to identify visitors personally and also to spot any potential intruders. If the cameras are connected to video recorders so that their views are intermittently recorded on tape, then any event that occurs at the home can be reviewed on the videotape later. This record of events, with the time recorded on the tape, is very helpful to police investigating a crime that occurred in the owner's absence and may even be instrumental in solving the crime. If nothing unusual is recorded on a tape, it can simply be reused.

Indoor/outdoor

The major difference between indoor and outdoor cameras is the housing. The outdoor camera needs to be able to withstand the weather extremes from below freezing to hot summer days. Some cameras are sold as indoor/outdoor and can be used in either location.

In addition, the outdoor camera needs to be able to adjust the exposure settings as the sunlight moves across the field the camera is covering, going from complete shadow, to full sun, to dark night. Indoor cameras need to be able to adjust from daytime lighting conditions to night lighting conditions, but the extremes are not as radical as they are for outdoor cameras.

Another difference is the cabling requirements for wired cameras. Outdoor wired cameras need to use cabling rated for outdoor use. Also, the wiring needs to be protected where it enters the camera housing and where it enters the building. It needs to be protected not only from temperature extremes and wet weather, but also from being cut.

Cameras, like most electronic equipment, don't like heat or water. This means that they should be kept away from direct sunlight, inclement weather, and sprinklers. Cameras can also be blinded by light sources shining directly into the lens. They should be located, as much as possible, so as to avoid this problem. Yard lights can usually be relocated or redirected so they don't shine into the camera lens. The direction of sunlight can't be changed, however, and may require careful positioning of the camera so that sunlight doesn't hit the camera lens during any part of the day. Remember that the sun's angle in the sky changes with the seasons. A camera safely in the shade of the eaves during July and August may be exposed by the lower angle of light in December and January. This phenomenon is significantly more pronounced in the country's northern latitudes (and is extreme in Alaska where the summer sun circles around the horizon), but it affects all areas to some degree. Reflected light coming off of a nearby window or the surface of a swimming pool can also blind a camera. So can car headlights entering the driveway or sometimes passing by on a curved street.

All of these possibilities should be checked and, to the extent possible, and when possible eliminated when placing video cameras.

Day/night

During the day, color cameras shoot in color. Many of these cameras then switch automatically to black and white mode when the lighting conditions become too dark to capture useful images in color. The cameras also often use IR illumination at night.

It is usually more important that the cameras function well in low-light levels than that they view in color. A black-and-white camera with high light-gathering capacity provides better images for identifying people and details than most color cameras, especially at night.

Fixed vs. animated

A fixed position camera is set up so that the same view is captured at all times. This is a less expensive camera. This is one of the most common and least expensive ways to set up a surveillance system. These are useful for monitoring stationary areas. It is also useful for monitoring high risk areas. This might include monitoring home entrances, rooms, and valuable objects.

Animated cameras are capable of covering more area. The camera is mounted on a device that allows it to pan, tilt, and zoom (*PTZ*). This could be manually operated or some can be configured to automatically pan and tilt on a regular or variable basis to cover more areas than can be seen with a fixed camera. These are more expensive and are more likely to be employed in a business environment where it is important to be able to follow a specific person as they walk through the building, customers as they leave a store, and areas such as gaming tables or large areas of a store floor.

If a video camera does have a panning motor attached, it needs to be hardwired to a power source, as the motor consumes too much power for long-term, battery-powered use. A stationary video camera can be battery-powered but still requires frequent battery changes or recharges. This is especially true if the batteries are exposed to high heat in an outdoor location, which tends to discharge them more quickly.

Surveillance

One of the most common uses of surveillance cameras is to aim a camera at entrance doors to the home. Not only does this provide the opportunity to catch intruders in the act, you can use it for seeing who is at the door. If you are working at home while waiting for the repairman to come and don't want to answer the door for just anyone who happens to come by, you can see who is at the door by viewing the image on the monitor or if your PC is equipped with the ability to view the camera image, then you can see who is at the door.

Another use for cameras is what are popularly referred to as Nanny cams. This is a camera that is aimed at a sleeping baby or a child at play. It enables you to keep an eye on the children without the need to be physically present in the room at all times.

Recording

Originally, if you wanted to record what was captured by your security cameras, the only cost effective method was to write it to video tape. The recorder for a video surveillance system should be a high-quality unit capable of recording all the resolution picked up by the camera. It should also have durable recording heads that are serviced frequently, as it will be in constant use recording images, most of which won't be of any value, but a few of which may be very important. These few need to be as clear as possible in order to reveal valuable details, hence the need for a recorder that records everything that the camera sees.

Digital video recorders (DVRs) are a cost effective method of recording the images. It can be a separate DVR device or it might be an application on a computer that records the information to the PC hard drive.

You can set up the recording of the cameras so that it only record when something triggers the signal to be recorded.

- Internal detection: Can be programmed to trigger recording when the scene changes. You can set the amount of movement required before recording is triggered.
- External detection: Might be connected to an alarm so that when the alarm is tripped recording begins. It might also be activated by a motion detector.

The recorder for a video surveillance system should be a high-quality unit capable of recording all the resolution picked up by the camera. It should also have durable recording heads that are serviced frequently, as it will be in constant use recording images, most of which won't be of any value, but a few of which may be very important. These few need to be as clear as possible in order to reveal valuable details, hence the need for a recorder that records everything that the camera sees.

The best recording unit is the type that records only one frame per second from the camera. This conserves videotape, allows the frames that are recorded to be of the highest quality, and permits up to a continuous week of surveillance to be recorded on a single tape. Alternatively, the recorder can be an extended time type that records 24 frames per second, but runs the recording tape more slowly so that up to 10 hours of surveillance can be recorded on each tape. This type doesn't record at the same resolution as the single-frame-per-second unit, and its tapes have to be changed daily.

Sequencing vs. multiplexing

Sequencing is when you record one camera followed by another camera. For example, if you have five cameras, it would record X-amount of time on camera 1, then move to camera 2, camera 3, camera 4, camera 5, then back to camera 1.

A multiplexer records all cameras at one time and tiles the images on the monitor. You can usually then switch to a full screen view of a specific camera's image when you need to. Depending on the software supporting the cameras and monitor, you might be able to record all of the cameras as separate video files or it might record all of the images together.

Do it!

C-2: Identifying camera applications

Questions and answers

- 1 Which factor is important for selecting a surveillance camera?
 - A Color instead of black-and-white
 - B Size of the camera
 - C Low-light functionality**
 - D All of the above
- 2 Panning motors:
 - A need to be hardwired to a power source.**
 - B work best on battery power so they can be placed anywhere.
 - C are too expensive for home users.
 - D none of the above.
- 3 Video surveillance recorders don't need to be very good since camera resolution is low anyway. True or false?

False
- 4 What are the advantages of using a recorder that captures images one frame per second?

Conserves tape, recorded frames are high quality, up to a week of surveillance can be recorded on a single tape
- 5 When is it recommended that a video monitor be used?

If the camera isn't connected to a recorder and if you want to monitor yard or entrances visually

Topic D: Security system peripherals and accessories

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
4.2	Describe basic security terminology and apply installation procedures and methodologies. <ul style="list-style-type: none"> Installation and Configuration of Security Panel <ul style="list-style-type: none"> Zone Types Delays Battery Backup and Power Supply Requirements

Installing a security system

Explanation

Standard security systems usually allow for up to eight zones and large-scale systems allow up to sixteen. Any system can have less than the maximum number of zones by simply not connecting devices to some zone monitoring circuits. Exhibit 5-10 shows a home floor plan divided into zones for a security system and possible locations for sensor devices within each zone.

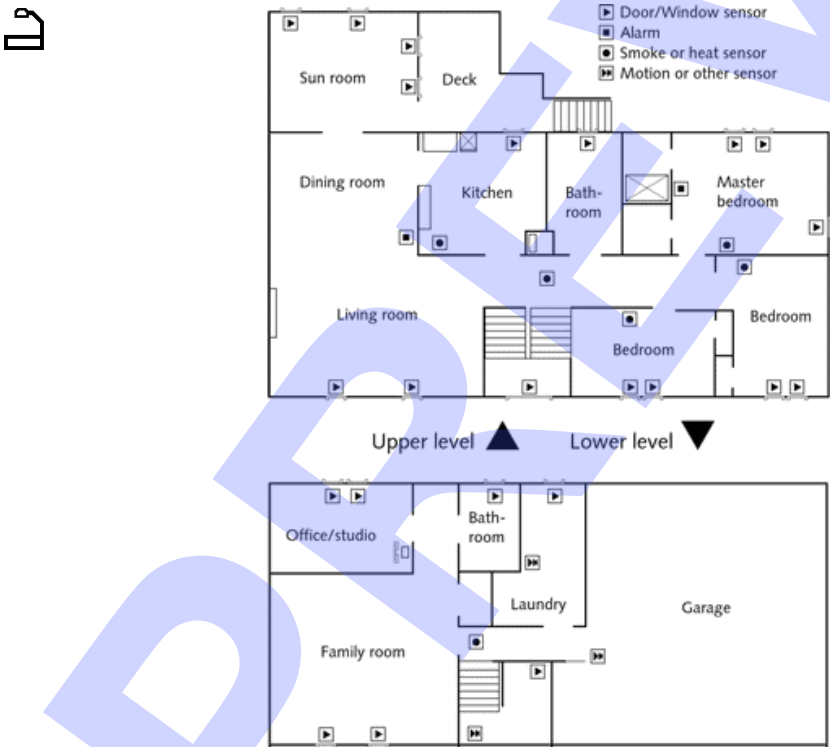


Exhibit 5-10: Home security system plan

Entry component installation

Using a variety of detection devices and sensors in the most vulnerable areas helps ensure that any attempt to break into the home immediately sounds an alarm and summons assistance. Exhibit 5-11 identifies the common entry points in homes where break-in attempts are made. Statistics shown in the following table are from ADT Security Systems and indicate the percentages of burglary attempts that are made for each entry point.



Exhibit 5-11: Common entry points for burglary attempts

Rank	% of break-in attempts	Location
1	34	Front door
2	23	First-floor window
3	22	Back door
4	9	Garage
5	4	Basement
6	2	Second-floor entry
7	6	Unlocked entrance and storage areas (not shown in Exhibit 5-11)

Security system components that would cover these entry points might include security cameras, magnetic switch window and door sensors, and glass break sensors. The installation requirements will vary based on manufacturer’s recommended installation procedures as well as whether you are using wired or wireless components.

*Do it!***D-1: Installing entry components**

Here's how	Here's why
1 Verify that the control panel is turned on and that the house and unit codes have been set	You will connect a door/window sensor and a motion detector to the control panel.
2 Install AA batteries in the Door/Window sensor	Many X10 components require batteries for the wireless components of the security system.
3 Place the two halves of the sensor with the arrows facing each other	This is the closed position for the sensor.
4 Hold the Test button down for a second	The red indicator will flash twice after you release the button indicating that a security code has been generated.
5 On the Security Console, set the switch to Install	
6 Press the Test button on the Door/Window sensor	The Security Console should beep to confirm that the sensor was recognized. The next available zone indicator should light up as well.
7 On the Security Console, set the switch to Run1	This is the usual operating position in which the console operates in silent mode. Run2 would sound the chime whenever an event occurred.

Interior component installation*Explanation*

If someone somehow gets into your home without setting off a door or window alarm, you can still detect intruders as they attempt to move about inside your home. One of those methods is using a motion detector.

*Do it!***D-2: Installing interior components**

Here's how	Here's why
1 Insert AA batteries in the motion sensor	The MS10A sensor requires four AA batteries.
2 Set the slide switch on the back to 2	This will trip the alarm only after two movements are detected. Setting it to 1 would trip the alarm after a single movement and could trigger false alarms.
3 Using a pencil or other small object, press the Code button in	It is located on the back of the MS10A motion sensor. This will set the device code.
4 Place the motion detector in a location where it cannot detect any movement	Face it to a wall or place a box over it. Motion during the installation could cause the device to install itself twice in the security system.
5 On the Security Console, set the switch to Install	
6 Press the Test button on the motion detector	A beep should sound from the console and the next unused zone indicator should light.
7 On the Security Console, set the switch to Run1	

Camera installation

Explanation

When installing cameras, you need to take into consideration where they are being installed and for what use you are installing them. The factors covered previously in this unit all need to be considered when you are selecting the cameras to use in your security system.

A good design has all outside areas covered by two cameras, if possible. This requires placing the cameras high up, away from visual obstructions. You also might consider using cameras that can pan (move back and forth) by remote control. A panning camera under the eaves of a home can often cover 270 degrees of the surrounding yard. With a camera on each corner of the home all areas of the yard are at least double-covered and some more. Double coverage of yard areas eliminates any blind spots that a single camera might have because of visual obstructions such as trees and other landscaping in the yard.

If cameras are also placed inside the home, double coverage usually isn't necessary, but the camera needs to be placed out of the way of visual obstructions. Inside cameras should also be concealed, if at all possible. Their obvious presence makes many people nervous and may cause a definite chill in the home's social atmosphere. Placing inside cameras in concealed locations within the home's decor lets them function without the drawback of making guests, or even the home's usual occupants, uncomfortable. Miniature cameras are now available that can be placed in books, ceramic pieces, picture frames, or other home furnishings. These devices can be easily relocated if the occasion requires, and they eliminate the need for any hole in the wall such as was once necessary to conceal a camera behind a one-way mirror.

If a video camera does have a panning motor attached, it needs to be hardwired to a power source, as the motor consumes too much power for long term battery-powered use. A stationary video camera can be battery-powered but still requires frequent battery changes or recharges. This is especially true if the batteries are exposed to high heat in an outdoor location, which tends to discharge them more quickly.

Configuring cameras

Some cameras are extremely simple. There is no configuration: You plug in the camera and that's all you do.

You might have to adjust the exposure to suit your needs if the camera has adjustments for exposure. If you are using a camera with built-in PTZ features, you might need to configure the range of motion and how fast or slow it moves. If you are using a camera that triggers recording of the signal, you will need to configure under what circumstances recording will begin.

Do it!

This is written using the X10 model WVK54 wireless camera kit.

A is an arbitrary selection, but must match that selected on the video receiver.

D-3: Installing and configuring cameras

Here's how	Here's why
1 Locate the camera/video sender, the receiver, RCA cables, and the remote controlled power supply	You will install a wireless camera with a video receiver.
2 Position the camera	If you are doing a permanent installation, you can attach it to a tripod or screw it to the wall. If you are installing it outdoors, you will need to drill a hole through which the low voltage power jack can be run.
3 Plug in the power supply jack into camera adapter cable	This is the power supply that has code wheels on it.
4 Connect the power supply to a power source	
5 Set the camera channel switch to A	The options are A, B, C, and D.
6 Aim the antenna toward the TV on which you will view images	
7 Set the Housecode dial to the letter on the control panel	These must match if you are going to remotely manage the camera.
Set the Unit code to an unused number	Each device needs a unique code.
8 Connect the RCA cables to the video receiver	Be sure to match the colors to the appropriate jacks.
Connect the other end of the cables to the TV	
9 Connect the power supply to the video receiver and to a power source	
10 Slide the power switch to the On position	It is located on the side of the video receiver.
11 Set the channel switch to A	It must match the channel selected for the camera.
12 Position the video receiver so that the flat side of the antenna faces the camera	It doesn't need to be in the same room, but does need to be oriented to pick up signals by positioning the antenna toward the sender—in this case, the camera.

Environmental sensor installation

Explanation



Environmental sensors are devices that react to some aspect of conditions around them. A temperature sensor, for example, continually sends the current temperature to the processor, which then determines whether to adjust heating, air conditioning, or other systems, based on the data it receives.

Examples of environmental sensors include:

- Heat (infrared) sensors
- Smoke detectors
- Water level sensors
- Chemical sensors such as carbon monoxide monitors
- Gas

All of these devices send data to the processor about the particular environmental condition that they monitor. The processor compares this information to its programmed instruction set and directs the system to respond accordingly.

Heat sensors, whether inside or outside, should never be placed where direct sunlight falls on them during any part of the day at any time of the year. They also shouldn't be placed where unusual heat from a fireplace or cooking appliance can reach them. Smoke detectors shouldn't be placed directly above a stove or oven where the occasional smoke or steam from normal cooking may trigger them. Placing such fire-warning devices a little distance away from heat and smoke particle sources can prevent constant false alarms but still give adequate protection from a genuine fire.

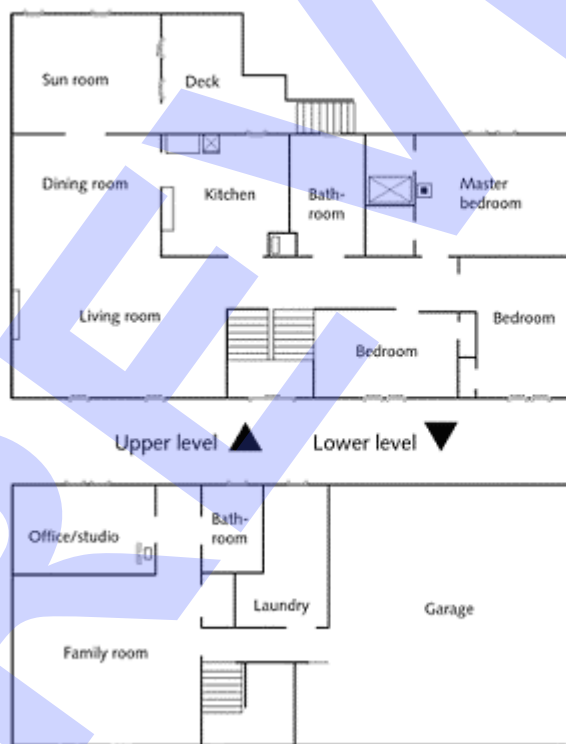
Homes that have natural gas service for heating can monitor that service by means of a *pilot light sensor* connected to the security system. The pilot light monitor can be either a light sensor or a thermocouple. In gas heating systems without continuous pilot lights, a pressure sensor on the gas line can be used to confirm that gas is still available for use. Another useful sensor in the area of a gas furnace or water heater, as well as a gas dryer or stove, is a gas detector that can warn of a leak in the gas system. The vast majority of gas leaks result from an appliance inadvertently left on, or from a crack or burn-through in the gas-fired heating element of the appliance. A gas sensor placed in the room where these appliances are located can quickly alert the security system of a problem.

Water sensors are of two types, both of which can be very helpful in avoiding water damage in the home. The first is a flow meter placed in the main water line to the home. This device can monitor the flow of water in the home's pipes and sound a warning if the flow is excessive or if water is flowing at all in the hours when it shouldn't be. By checking the flow meter for the early morning hours, say from 2 until 4 a.m. when no water would normally be flowing in most homes, even fairly small leaks in bathroom fixtures can be found and corrected. A flow meter is very helpful in detecting water loss in leaking sprinkling systems as well.

The other type of water system sensor is simply a device that detects the presence of water where there shouldn't be any. Water sensors placed in dry areas or a basement can warn of a broken pipe or leaking appliance before serious damage is done. If the home is in an area where ground water is a problem, a basement sensor can alert the homeowner to incoming water as soon as it appears. If the problem is pervasive enough that the home has a sump pump, which is a self-starting pump installed in a pit below floor level to keep ground water out, then a water sensor is a necessity as a backup for the pump in case it fails mechanically or from lack of power.

*Do it!***D-4: Installing environmental sensors**

Here's how	Here's why
<ol style="list-style-type: none">1 Using the floor plan shown, indicate where you would place heat sensors by placing an H on the floor plan2 Indicate where you would place smoke detectors by placing an S on the floor plan3 Identify where you would place carbon monoxide detectors by placing a C on the floor plan4 Indicate where you would place gas sensors by placing a G on the floor plan	You will identify where to install environmental sensors throughout a home.



System testing

Explanation

Testing ensures that the security system is working under the actual range and obstruction conditions of the home. If either a sensor or the security panel is relocated, testing should be done again to be sure that all transmissions can still be received. If it's the security panel that's moved, all sensors should be retested.

If sensors and the control panel are in place and equipped with batteries, the sensors should all be tested to be sure their signals reach the control panel correctly. The testing should be done before the call-in dialer is connected so that accidental alarm signals won't trigger a call.

When the sensors are confirmed to be working correctly, the call-in dialer can be connected to the telephone line and programmed with the numbers it's to call and the message to be recited. The call-in dialer can be tested by programming it with the telephone number of another line to the home or to the home of a friend who can be made aware of the test beforehand. With only the one call number programmed, test the system by triggering an alarm from one of the sensors to see if the call-in dialer performs as intended. If it does, the test number can be deleted and replaced with the permanent call-in numbers the system is to use.

Wireless sensors should all be tested to be certain that they're within range of the receiver in the security panel. If any aren't, an auxiliary receiver can be installed at a wall outlet within range of the wireless units. The auxiliary receiver can then relay the wireless transmissions via the AC wiring to which it's connected.

System service and maintenance

Security systems rarely break down. Their reliability is partly a function of good initial construction to meet the durability requirements of a quality system and partly due to the fact that their components have few moving parts and a very low level of activity. They simply observe and occasionally signal conditions around them. Security system components almost never wear out. Most service and maintenance for these systems center on their aging rather than mechanical or electronic breakdowns.

Security sensors are self-monitoring, sending a signal to the security panel periodically to confirm their functioning status. They also monitor their batteries and signal when power begins to drop off. Finally, if the condition that a sensor is monitoring changes or something happens to the sensor to impede its monitoring of that condition, it signals an alarm. With this degree of self-monitoring, little external monitoring of sensors is ever needed. As long as their batteries are changed when signaled as low, sensors can function almost indefinitely without service.

Security panels also require little in the way of service or maintenance. They're generally AC-powered and have backup batteries that age over time. These should be changed every two to three years, even if never used. Like all electronic equipment, security panels can be damaged by power surges and spikes and should be protected by a surge suppressor on the AC circuit.

The response devices in a security system are the most vulnerable to maintenance problems and should be tested annually to see that they're still functioning well. Electronic speaker alarms rarely malfunction, but mechanical bells do and should be activated to confirm that they're working. The same is true of any mechanical response device that functions only if an alarm is signaled. Electric solenoids, motor-driven actuators, and especially valves, left unused for a year or more, can corrode and become frozen in their static position. They should all be activated periodically to be sure that they can activate when signaled to do so by the security panel.



As is the case with all electronic systems, the enemies of electronic security systems are heat, dirt, power spikes, and water. Wherever any of these can attack a part of the system, it should be protected as much as possible and regularly monitored for possible failure. Among the specific points in a security system that should be checked are:

- Wireless window detectors (for heat damage to the transmitters from sunlight coming through the glass)
- Outside motion sensors (for dirt or obstructions that may block all or part of their fields)
- Inside motion sensors (for dust and spider webs blocking their fields)
- Outside wireless sensors (for weather damage)
- Break switches on window and door sensors (to detect anything inserted in the switch to prevent its opening)
- Make switches on pressure pads or similar devices (to detect anything inserted in the switch to prevent its closing)
- Locks (to be sure they don't stick open)

Do it!

D-5: Testing the security and surveillance system

Here's how	Here's why
<ol style="list-style-type: none"> 1 Verify that all components are plugged in to power sources, have batteries installed, and are turned on as needed Verify that the controller is set to Run1 mode 2 Walk in front of the motion detector 3 Walk in front of the surveillance camera 4 Open the magnetic contact 	<p>You will test the installed components of the security and surveillance devices you set up.</p>

Unit summary: Security and surveillance systems

- Topic A** In this topic, you learned about the different types of **security peripherals and accessories**. These include motion sensors, glass break detectors, magnetic contacts, smoke and fire detectors, environmental sensors, vehicle detection, microwave beam detectors, pressure sensors, sirens and strobes, security keypads, keyfobs, and panic buttons. Lastly, you defined several **security monitoring formats** including SIA, Contact ID, 4/2, and 3/1.
- Topic B** In this topic, you compared and contrasted the two types of **security infrastructure**: wired and wireless. A wired infrastructure utilizes 22/4 and 22/2 wire to connect each of the detectors and keypads from the main alarm box. You learned about the use of power supervision relays, end of line resistors, polarity reversal relays, and line seizure devices. Next, you learned about the different types of **access control devices** including keypads, card readers, biometrics readers, door strikes, electronic deadbolts, and magnetic locks. Then, you examined the Wiegand protocol. Lastly, you installed a **security panel**. You learned about the concepts of zone types, delays, battery backups, and power supply requirements.
- Topic C** In this topic, you learned about the three types of **security and surveillance cameras**. They are IP, analog, and hybrid. Next, you learned about **camera specifications** including lens type, lux rating, resolution, black and white, color, IR illumination, and power consumption. Lastly, you identified several applications for security and surveillance cameras including use indoors and out, during night and day, from a fixed position, from an animated position, surveillance, recording, sequencing, and multiplexing.
- Topic D** In this topic, you installed a security system. You went over how and why you install entry components, interior components, cameras, environmental sensors, and smoke and fire detectors. Lastly, you learned how to test the security and surveillance system.

Review questions

- 1 What is a zone in a security system?

A zone is a defined area in a home protected by one group of sensors connected to one segment of the security panel.

- 2 A video camera in a security system is wired to a monitor or switch panel using what type of cable and connector?

- A Category 2 with RJ-45 connectors
- B composite video cable with RCA connectors**
- C Category 5 with RJ-45 connectors
- D MIDI cable with USB connectors

- 3 What does arming a security system for outside or away status mean?

This is the arming status for when all occupants are out of the home, and it's unoccupied. All security sensors inside and outside the home are activated for maximum security.

- 4 When a security panel receives a breach signal from a sensor, what does it normally do?

Sound an audible alarm and activate a call-in device to summon emergency assistance. It may also initiate other actions.

- 5 Statistics show that most burglary attempts are made at what three entry points: _____, _____, and _____.

front door, first-floor window, back door

- 6 Motion sensors' locations should take into account what factors?

Avoiding obstructions that could shield an intruder, avoiding placement where a shield could be placed in front of them, avoiding placement in hot outdoor settings where they won't work well, avoiding placement where non-threats, such as falling leaves, blowing debris, or drifting snow could trigger false alarms.

- 7 Why is double coverage of video cameras in a yard a good security practice?

It eliminates blind spots produced by obstructions in front of a single camera. It also provides backup in case of camera failure or destruction.

- 8 The normal state of a break switch sensor is _____.

closed

- 9 The central control device for security systems is the _____.

control panel

- 10 How do security sensors monitor themselves?

By sending a signal to the security panel periodically to confirm their functionality. Battery-operated components signal when power drops off.

Independent practice activity

You will install an outdoor motion detector with floodlights. This is written to use X10 model PR511. You will also install a remote chime (model SC56A) so that when the motion detector detects movement, the chime will sound.

- 1 Turn off power to the junction box where the motion detector will be installed.
- 2 Install the gasket onto the junction box and thread the house wiring through the gasket.
- 3 Connect the green wire from the mounting plate to the bare ground wire in the junction box. You could install it to the ground screw if one exists.
- 4 Using a wire nut, connect the white wire from the motion monitor to the house wiring white wire. Verify that no bare wires are exposed from the wire nut.
- 5 Using a wire nut, connect the black wire from the motion monitor to the house wiring black wire. Verify that no bare wires are exposed from the wire nut.
- 6 Fasten the mounting plate to the junction box.
- 7 Insert a light bulb into each lamp holder, securing the insulating ring in each lamp.
- 8 Unscrew the bottom of the monitor to expose the control settings panel. Set the Dusk control to Light.
- 9 Set the Range to Max.

- 10 Set the Time Delay to 0.1. This will provide a 6-second time delay.
- 11 Position the sensor head to the area to be covered, making sure the sensor head remains level to the ground.
- 12 Position the floodlights as desired.
- 13 Turn on power and wait one full minute.
- 14 After one minute, walk into the sensor area. The lights should come on and remain on for 6 seconds after no more movement is detected.
- 15 Set the Dusk control to the index mark.
- 16 Set the range control to the desired setting. Max will increase the range; Min will prevent it from sensing traffic, pets, or small animals.
- 17 Set the sensor to floodlights so that the lights turn on when motion is detected.
- 18 Set the Housecode to match the controller code.
- 19 Set the Start code to a unique number. On this unit, the Start code is equivalent to the Unit code.
- 20 On the Remote Chime set the Housecode to the letter of your X10 controller.
- 21 Set the Unit code to the same number as the floodlights.
- 22 Plug the remote chime into a power source.
- 23 Walk past the motion sensor to verify that the chime functions properly.

Unit 6

Home control and management

Unit time: 180 minutes

Complete this unit, and you'll know how to:

- A** Identify methods used to integrate control subsystems.
- B** Describe basic HVAC terminology and install peripheral control devices.
- C** Describe basic lighting terminology and install peripheral control devices.
- D** Identify and install component power protection devices.

Topic A: Control systems integration

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
5.2	Define and recognize control systems that integrate subsystems in the home. Describe their functionality, characteristics, and purpose. <ul style="list-style-type: none"> • Embedded control systems and Personal Computer (PC)-based control systems
5.1	Identify user interfaces and their appropriate applications <ul style="list-style-type: none"> • Device types <ul style="list-style-type: none"> • Remote controls • Keypads • Touch screens • Keyfobs • Telephones • SmartPhones • Cell phones • PDAs • Web tablets • Personal computers • Laptops • Describe the importance of simplicity and ease of use as it pertains to the end user
5.3	Identify commonly used communication protocols and their applications. <ul style="list-style-type: none"> • IR • Serial • IP • RF • Bluetooth • Contact closure • Inputs (zones) • Z-Wave and Zigbee • ASCII • Proprietary protocols

Embedded control systems

Explanation



An *embedded control system* is a device that contains only the computer functions needed by the device. They are often dedicated to performing a single task. Some are small, fitting all of the functions on a single chip—basically a computer on a chip. Other systems are composed of multiple devices including networking features and peripherals all enclosed in a single box.

The embedded control system is often built into the device that it controls. In these cases, it is usually known as *firmware*. Some devices have no user interface, while others, for example PDAs, have a user interface similar to a PC desktop. In between those two extremes are devices that use buttons or a small display to select options.

Many devices use pieces of the Linux operating system. This helps ensure interoperability with other devices which also use Linux as the embedded control system operating system.

If the device has the ability to have an IP address assigned to it, this also increases its compatibility and interoperability. This enables use of devices over a home network. It also even provides the possibility for remote access to devices over the Internet.

Sometimes an organization composed of reps from various companies will develop a standard to ensure interoperability of devices between the various companies.

Manufacturers often have standards to which they design their systems. If you purchase all of the components from that company or buy components that are manufactured to meet those standards, then they will be compatible. However, if the company doesn't make a component you want, then if you purchase a device outside this standard, it probably won't be interoperable with the rest of your components.

For example, if you are installing an X10 system, then it won't interoperate with a wired security system that doesn't have embedded controls for communicating with X10 wireless devices.

PC-based control systems

A PC can often function as a control system interface to integrate various subsystems in the integrated technology arena. For example, a Windows Media Center PC can integrate all of your audio/video systems. This same PC could also be included as part of an X10 controlled security and control system. This could be a desktop PC, a laptop, or a SmartPhone. A SmartPhone is usually a cell phone with PDA functionality running an operating system such as Windows CE, Symbian, RIM, or Linux.

User interfaces

There is a wide variety of devices that can be used to control components of your integrated home network. Many users want more control over devices than the control capabilities built into a specific controller. By using a PC or other sophisticated control panel, you can create macros or sequences of commands to increase the functionality of a controlled device.

The simplest control is just using the built-in features of a controller device. Using other user interfaces can be nearly as easy or it can be quite complicated. It all depends on what you are trying to do, the components you have available on your network, and your tolerance for learning new skills. A set of well written documentation for a control device makes it possible for almost anyone to get a user interface device to function as you need it to work.

Remote controls

Many subsystems come with a dedicated remote control. For example, your TV, your DVD player, and your audio receiver all came with remote controls. In addition, your media PC probably came with a remote control as well. Even gas fireplaces might have a remote control.

Universal remotes enable you to combine the function of several different remotes into a single device. Some models require that you enter codes to identify the brand and model of the equipment you want to control. Other models are learning remotes which can be taught to perform the functions of the original remote.

X10 systems can be set up to use a remote control as well. You can do things such as turn lights and appliances on and off with the remote as well as dim or brighten the lighting. Exhibit 5-1 shows an example of an X10 remote control. This can be used to interface with TV, audio, cable, and PC in addition to X10 devices. Just as you can select to use it with the TV or with the DVD player, there is also a button to select that you want to control a device connected to the X10 network. The channel up button turns on an X10 controlled device and channel down turns it off. Volume increase button brightens a lamp and the Volume decrease button dims a lamp. The power button in the upper right turns on all lights. The “M” button turns all lights off.



Exhibit 6-1: An X10 hand-held remote control

Keypads

In an HTI system, keypads are used to arm and disarm the security system. Keypads can be located near the home's entrances where they are used to arm and disarm the security system. They might also serve as input devices for the codes to open cipher locks on doors. Other keypads can be located throughout the home and may control entertainment systems, lighting, curtains and shades, garage doors, and others functions.

Keyfobs

Keyfob devices are typically just used for arming and disarming alarm systems, opening doors, or summoning emergency help using the panic feature. However, some can also be taught additional functions to control other devices.

Phones

Some systems, and in particular X10 systems, can be controlled using a telephone. Installing an X10 phone interface device enables you to call into the X10 network using a Touch Tone phone to control devices on the X10 network. These devices enable you to access the network remotely or to use a phone inside the house to control devices. Some models also announce back to you the command you performed so that you know that the command was carried out.

Cell phones and SmartPhones don't use Touch Tone signaling. However, some systems are now providing voice support for their networks, so these phones should work just fine for connecting to the network.

Touch screens

Touch screens are LCD screens that contain a touch sensitive surface. By touching the screen you make selections. You can program a sequence of commands to perform with a single touch of the screen. These are often universal remote control devices that enable you to control a variety of devices throughout the home from a single controller.

Web tablets

A Web pad (also sometimes known as a Web tablet) is a wireless single-purpose device designed to simplify and enhance Internet connectivity. A Web pad consists of a wireless portable pad with an LCD screen and a base containing a wireless transceiver that sends and receives data from the portable pad. The base unit is connected to the Internet and through its wireless link, the Web pad can send and receive data over the Internet.

Web pads have gained some acceptance in the marketplace, but their single function use and relatively high cost due to the wireless technology and LCD screens they use, has limited their sales. The best units include a serial port, a USB connection, a wireless network card, and often a SmartCard slot (more commonly used in Europe than in the U.S.), as well as a selection of wireless drivers and Internet software tools.

Do it!

A-1: Installing a PC-based control system

You should have received an e-mail link to download the software prior to class.

Here's how	Here's why
1 Install the ActiveHome Pro software from the location specified by your instructor	You will use ActiveHome software and 2-way PC interface as a controller.
2 Connect a USB cable to the Active Home Pro 2-Way PC Interface	
3 Connect the USB cable to the PC	
4 Plug the ActiveHome Pro module into an electrical outlet	
5 Connect a lamp to a Lamp Module	To install a device that can be controlled.
Set the House Code to match the Control Panel	The control panel was previously set up.
Set a unique Unit Code	
Plug the lamp into the Lamp Module and turn it on	Devices should start out in the on position.
Plug the Lamp Module into an electrical outlet	

Control system user interfaces

Explanation

A variety of user interfaces can be used to interact with various home control devices. Some of the home subsystems that you might want to control include the A/V components and the security system. In addition, you might want to control lighting, heating and cooling systems, lawn sprinklers, window and door opening and closing, and window treatments.

The appropriate device for controlling all of those components might be done from a single device such as a computer or laptop. It might also be possible to configure a PDA, a cell phone, or a regular telephone to remotely control devices.

Most can be controlled by a remote control device designed for the system. These systems usually also include keyfob and keypad devices to access and control the various subsystems. In X10 systems, a remote control similar to those used to control TVs and DVD players can also be used.

Touch screens, Web tablets, SmartPhones, and cell phones are gaining the ability to also be integrated into home control systems. This usually requires special programming to make the devices aware of the devices which you want to control.

*Do it!***A-2: Using a PC as a control system user interface**

Here's how	Here's why
1 Open the ActiveHome Professional application	You installed the ActiveHome software and it might already be open. You previously installed a security control panel and connected a motion detector, surveillance camera, and door/window sensor.
2 On the Rooms bar in the left panel click the + icon Enter Room# Click OK	The Add a Room dialog box is displayed. Where # is your lab number. Under Rooms in the left panel your new room is listed.
3 Right click Room# Choose Add Module	The Add a Module dialog box is displayed.
4 In the Name of the new module text box, type Lamp# From the Type of Module drop-down list, select Lamps From the Module drop-down list, select Lamp Module Verify that the Create in room text box displays your room Set the House Code and Unit Code to match the settings on the Lamp Module Click OK	To name the module. This is the category of module you will control.
5 Click the On/Off switch icon twice	The Lamp# interface is listed under All Rooms in the upper right panel. It starts in the off position, so you need to turn it on, then off to turn the light off.

Communication protocols

Explanation

In order for components in a smart home to communicate, they need to all talk the same language. This is known in the computer and electronics world as using a common protocol. Being able to communicate between devices or to a central control panel requires that all devices use the same protocol.

IR

The IR protocol is a relatively simple protocol. This protocol requires the sender to send a series of start flags before sending the data packet which can be up to 16 bytes in length.

Infrared wireless technology uses pulses of invisible infrared light to transmit signals between devices. It offers relatively low-speed, line-of-site connections between devices. Infrared light cannot pass through obstructions or around corners. Connection speeds range from 9,600 bps to 4 Mbps with a typical maximum range of 10–20 feet. To make connections, devices must aim their transmitter/receivers directly at each other. Devices that are more than 45 degrees off to the side of a receiver will generally be unable to connect.

The most popular form of infrared wireless is the Infrared Serial Data Link (ISDL) technology, which offers a wireless serial connection at 1.5 Mbps with a maximum range of 20 feet. Laptops and PDAs with infrared ports typically implement ISDL infrared.

Devices that use infrared include handheld computers, such as PDAs, and occasionally wireless keyboards, mice, and printers. Infrared connection technology standards are set forth by the Infrared Data Association (IrDA). Exhibit 5-11 shows an IrDA infrared port on a laptop. IrDA is a computer protocol and is not usually used for things such as remote controls.

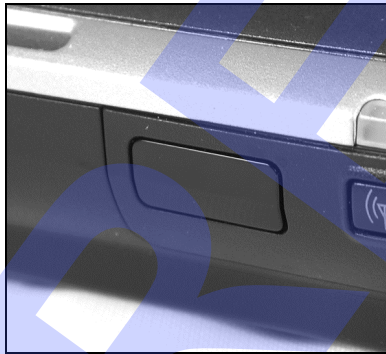


Exhibit 6-2: An IrDA infrared port on a laptop

Radio

Radio-based wireless communications use signals sent over electromagnetic radio waves to transmit data between devices. Radio transmissions can pass through most non-metallic obstructions and around corners. Thus, it is not a line-of-site technology. Radio transmission offers moderate to high-speed local and wide area connections.

Various radio networking technologies have been developed. Currently, the most common of these include 802.11b and 802.11g. They offer up to 10 Mbps business or home networking and Internet connectivity over modest distances.

Radio networking technologies are sometimes called RF (radio frequency) technologies. RF devices have antennae, but they might be hidden inside the device. For example, a laptop's IEEE 802.11g wireless network adapter antenna is typically hidden in the laptop's case.



Exhibit 6-3: An IEEE 802.11g wireless router

Bluetooth

Bluetooth is a short-distance radio communications technology developed by the Bluetooth Special Interest Group, which includes over a thousand companies. Chief among these are Siemens, Intel, Toshiba, Motorola, and Ericsson.

Bluetooth is designed to enable devices—such as cellular telephones, PDAs, personal audio players, PC peripherals, and PCs—to discover the presence of other Bluetooth devices within range. Once detected, these devices self-configure and begin communicating. With Bluetooth devices, you shouldn't have to configure any communications parameters, such as network addresses.

Bluetooth devices have antennae, which are usually hidden inside the device. A cell phone that supports Bluetooth probably has an external antenna that's used for both the cellular telephone communications and Bluetooth connectivity.

Bluetooth devices operate in the ISM (Industrial, Scientific, and Medical) radio band. A Bluetooth device can connect with up to seven other Bluetooth devices. The devices connect via a piconet. (A *piconet* is a network of devices connected in an ad hoc fashion through Bluetooth technology.) Devices have a 48-bit device address. The IEEE assigns the first three bytes of the address to a manufacturer. The remaining three bytes are available to the manufacturer to create unique identifier addresses for each device.

To create the piconet, devices discover each other by searching the area for other Bluetooth devices. A device can operate in discoverable mode, so that other devices can easily find it, or in non-discoverable mode. Using non-discoverable mode helps you protect information from unauthorized users.

Bluetooth devices fall into three classes, based on the range of the devices. Most devices are Class 2 devices with a range of 10 meters. Class 2 devices operate at 2.5 mW. Class 1 devices have a range of only 1 meter, and Class 3 devices have a range of up to 100 meters. Class 1 devices are typically industrial-use devices.

An example of a Bluetooth device is shown in Exhibit 6-4. In this example, the mouse is turned over to show the Bluetooth address printed on the underside. The light on the front of the Bluetooth hub indicates that it's ready to receive a signal from another Bluetooth device. In this example, the hub is also the recharging base for the mouse. The hub connects to the computer via a USB cable.



Exhibit 6-4: A Bluetooth mouse and hub

Serial

Serial transmission is a technique in which bits of data are sent one at a time across the transmission medium. You could imagine the bits marching single-file down a single data-transmission wire (or across a single wireless transmission channel). Special sequences of bits delineate data from associated control information, such as marking the beginning and ending of bytes or blocks of data.

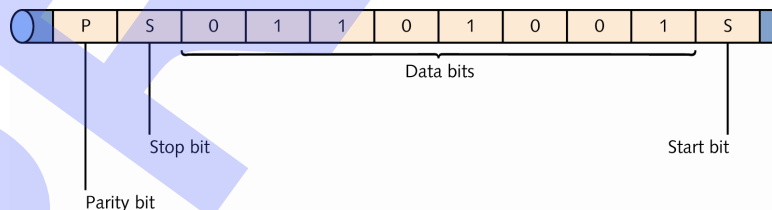


Exhibit 6-5: Serial transmission

IP

Communication between networks requires that they use a common protocol and that each computer or other device attached to each network have a unique address. The most common protocol currently used on LANs and to connect networks is Transmission Control Protocol/Internet Protocol (TCP/IP). This protocol is used throughout the Internet. TCP/IP addresses each node on a LAN by a unique Internet Protocol address (IP address), which consists of four numbers separated by periods; for example 192.168.2.23. Each of the four numbers in an IP address must consist of no more than eight bits of binary data, which means that each number cannot be higher than 256. This keeps the addresses short and standardized for consistency.

The Internet is really a vast collection of WANs, all interconnected to one another and able to communicate with each other. Data going from a node on a home LAN to a node on a distant network reaches its destination by traveling through the communication lines of other networks located between the originating point and the destination. There are usually many possible routes the data can take. Some are long and require more time for the data to arrive than others, but since all the WANs that make up the entire Internet are connected, it is possible to send data from a node on any LAN to a node on any other, provided the IP address of the destination is known and the data is directed toward that address by the Internet's data management devices, or routers.

Contact closure

Contact closure is a standard used in alarm systems. It enables you to easily monitor and manage alarms for things such as temperature extremes, water sensors, door sensors, and power failure sensors.

The alarms are composed of events and actions. Another way to say this is that they are composed of triggers and responses. Events are changes in the status of the contact closure. This might be a change between opened and closed or high and low voltage limits. You can define the actions to be performed when a trigger is activated. The actions might include calling a pager or phone number, sending a serial message, sounding an audible alarm, or sending an SNMP message.

When the action is triggered, the message that is sent includes information about the time and date of the event, the alarm name, and if desired, a user defined message that has been set up previously. Serial ASCII text strings that are generated when the alarm was triggered can be captured and sent using one of the previously mentioned communication methods.

Inputs or zones

Inputs and devices that provide input into a system need to adhere to the protocol standards used by the network or control devices. If they don't they won't be able to work with the system.

Some communication protocols require that devices be divided into zones. This enables the system to address all of the devices within the zone as a group. In a security system, having zones lets you know in which area of the home the breach of security occurred.

Z-Wave

The Z-Wave standard is a wireless standard designed for home automation networks. It was designed by the Zensys Company and the Z-Wave Alliance. The Alliance is a consortium of multiple independent manufacturers who all agreed to build components compatible with this open standard.

The standard operates in the ISM band. It has a range of about 100 feet, but building materials can reduce this range. It functions at 9,600 kbps. It supports up to 232 devices. If more devices are needed, multiple networks can be bridged together.

There is no master device in a Z-Wave network. It uses a mesh topology in which any device, also known as a node, on the network can communicate with any other device. If a device is too far away, devices between the two devices that are too far apart function as repeaters in order to get the message to the device.

ZigBee

ZigBee is a wireless communication protocol suite that makes use of low-power powered digital radios. It is based on the IEEE 802.15.4 standard. It operates in the ISM radio frequency band.

The ZigBee protocols are designed for use as embedded applications in lower power, low-data-transfer-rate devices. It can be used in devices to control things such as lights, HVAC systems, and security systems.

The protocol creates ad-hoc networks. Networks are either beacon-based or non-beacon networks.

Non-beacon networks have continuously active nodes which require more power than a beacon network. It uses the CSMA/CA channel access method. In other words, it waits until no other devices are active on the network before sending.

In a beacon network, routers send beacons out to nodes on the network periodically. Nodes can sleep between beacons, thus reducing power consumption. CSMA/CA is not required on beacon networks since the beacon is sent out on a regular basis.

ASCII

The Associated Standard Code for Information Interchange (ASCII) is the 7-bit code used by computers and other communications equipment to represent letters, numbers, and special characters.

The codes are represented in binary format, but are usually referenced by their decimal equivalent. The first 32 codes from 0 to 31 are control codes. For example, 10 is a line feed, 12 is a form feed, and 13 is a carriage return.

The printable characters begin at 32 and go up to 126. This includes punctuation and special characters, numbers, uppercase letters, and lowercase letters. A table showing all of the ASCII codes can be found at www.asciitable.com.

The Extended ASCII set uses an 8-bit code to include not only the codes designated for the ASCII character set. It also includes additional codes for characters used in languages other than English as well as graphics characters.



Proprietary protocols

Proprietary protocols are also known as closed source protocols. This is because the structure of the protocol is not shared as it is with open source protocols. Some proprietary protocols are very specific and only apply to a small installed base. Others are very widely applied. Any two users who agree on how to communicate can create a protocol. This would be a very small install base. An example of a more widely applied closed protocol would be the Skype protocol used in Skype VoIP applications.

Proprietary protocols can sometimes provide more features and functions than open source protocols. When a company develops a protocol that is specific to their devices, they can closely control exactly what the device can and cannot do.

Using proprietary protocols makes it difficult or impossible for other companies to develop products or applications that work with devices that use the protocol. This closed source gives the creators more control over how the protocol is used and can protect it from attacks.

Proprietary protocols do not interoperate with other products unless the creator decides to make the edges of the protocol available to others. If they do this, then other developers can write code or create devices to connect to the edges of the closed protocol.

The phrase “security through obscurity” can certainly be applied to proprietary protocols. Hackers are not usually going to devote time to a protocol that won’t get them into other systems.

Do it!

A-3: Examining control system communication protocols

Here's how	Here's why
<p>1 Using a search Web site, locate security systems, HVAC systems, lighting systems, and A/V systems that use each of the following protocols</p> <p>Zigbee</p> <p>Z-Wave</p> <p>RF</p> <p>Proprietary</p>	<p>You will identify subsystems that use various communications protocols.</p>
<p>2 Desktop PCs typically do not have such ports, though laptops typically do.</p>	<p>Desktop PCs typically do not have such ports, though laptops typically do.</p>
<p>3 Examine the infrared wireless device provided by the instructor. What issues might arise as you use such a device?</p>	<p>Infrared wireless is a line-of-sight technology. One of the biggest issues with using it is obstructions. Papers on your desk, dirt on the infrared lens, and other such common problems can prevent connections.</p>
<p>4 If your PC has an infrared port, turn on the infrared device and bring it within range of the PC's receiver</p>	<p>If your devices connect, you should see an indicator, in the status-bar area of the screen, that the device has been detected.</p>
<p>5 How far can you move from the PC before you lose the infrared connection?</p>	<p>Exact distances will vary based on the devices you're using. But in general, infrared wireless is limited to 10–20 feet.</p>
<p>6 Examine the radio wireless device provided by your instructor</p>	
<p>7 Does it have a visible, obvious antenna or more than one antenna?</p>	<p>Answers will vary.</p>
<p>8 If you have used a wireless network, share your experiences with the rest of the class. For example, where have you used it? Did it work well? From how far away could you connect? Did particular objects in the area cause interference?</p>	<p>Power lines, circuit-breaker panels, refrigerators, and other motorized equipment can cause enough radio interference to prevent RF wireless networks from functioning. Additionally, speed on these networks decreases fairly rapidly with distance.</p>

Provide students with a selection of infrared, RF, and Bluetooth wireless devices.

If software is required for the operation of these devices, provide that as well.

If you don't have any Bluetooth devices, ask students if their cell phones support it and get them to connect to each other.

- | | |
|----|--|
| 9 | Examine the Bluetooth wireless device provided by your instructor |
| 10 | Do the Bluetooth devices have a visible, obvious antenna or more than one antenna? |
| 11 | Can you connect to other Bluetooth devices in the classroom? |

Your cellular telephone or PDA might support Bluetooth. You could examine it instead.

Answers will vary.

Topic B: HVAC control

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
5.4	Describe the basic HVAC (Heating Ventilation and Air Conditioning) terminology and install peripheral control devices. <ul style="list-style-type: none"> Control layer <ul style="list-style-type: none"> Compatibility Communication layer <ul style="list-style-type: none"> Compatibility IP based, wireless, serial, and proprietary Zones HVAC <ul style="list-style-type: none"> Master slave configuration Microprocessor controlled configuration Programmable thermostats Importance of referencing manufacturer specifications and compatibility

Control layer

Explanation



The control layer is responsible for connecting the I/O points with local control. It allows you to interface with the HVAC equipment. In this way, you might be able to tie control of your HVAC equipment in to a single control interface that includes other subsystems. Being able to control the thermostat, the lighting, and the A/V systems from a single button press on a remote control device would certainly be a nice feature for you to be able to use after a long day at the office. It would also be beneficial to those with limited mobility who could benefit from setting these conditions with a single command.

Some of the functions that you might want to control include.

Function	Description
Delayed start	Delays starting the heating or cooling system when the weather is mild.
Optimum start	Starts the heating or cooling system to bring the building to a comfortable temperature by a specified time.
Night setback	Reduces the temperature to a lower setting overnight.
Anti-cycling	Delays starting the heating or cooling system to attempt to reduce frequency of cycling on and off. This may sacrifice comfort or performance of the system.

Whether the controller is centralized or connected directly to an HVAC system, the controller is usually programmable. You can create control program coding to customize the system for your needs.

Digital input/output controls usually are for starting and stopping the equipment. Analog input/output controls usually are used to check voltage or current signals and based on the results, control the movement of the heating or cooling medium control devices such as valves and dampers.

Communication layer

The communication layer of a HVAC control system is responsible for integrating data from I/O points and providing features such as alarm management and data collection.

Compatibility

The compatibility of components is vital to the smooth operation of a HVAC system. If there are different manufacturers' components you must find out if they will all operate with the chosen control and communication system. You may find some manufacturer's components use proprietary controls while others can be interfaced easily with your system. Be sure to refer to manufacturer specifications when purchasing components for the system to ensure that they are compatible with the control system you have installed.

Communication methods

There are four general ways the communication layer can be configured. These include:

- IP based system with Cat5 cable connectivity. This type of system uses off the shelf IP components which are universally available. Applications can be installed on a computer to access the HVAC system through a Web browser.
- Wireless model, with ease of set up as its strong point. This usually uses an IP address as well, so applications can be installed on a computer to access the HVAC system through a Web browser.
- A serial system uses a serial data cable. This typically connects directly to a PC that contains the control application.
- Proprietary systems used by the specific brand of HVAC components you are using. The down side is the incompatibility with components of other manufacturers. These systems usually use custom applications, so require that the operator learn another programming language or method to program the controller.

HVAC zones

The purpose of heating zones is to distribute heat more evenly and efficiently throughout the home. The two factors that make zones necessary in many home HVAC systems are distances from the central furnace to some parts of the home and the effects of outside climate, mainly sunlight.

In an HVAC system, the further heated air travels from its source (the furnace), the more heat is lost in transit, so that less remains when the air finally reaches its destination. The same is true for the cooled air from an A/C system. It warms as it moves through the ducts, absorbing heat from them as it moves. In a home with only one zone and relatively equal heated air distribution to all rooms, this results in the rooms closest to the HVAC system being the warmest, and those furthest away being the coldest. If colder rooms are brought up to normal temperature, warm ones are then too hot for comfort and vice versa.

Radiant heating systems with only one zone also have this problem. The heating water cools more by the time it reaches the most distant pipes than it does before reaching the nearby ones. The result again is uneven heating.

The A/C system suffers from a similar unequal heat distribution. However, this time it's caused by cool air from the air-conditioner warming more as it travels to the outer parts of the home than it does for those nearer. This causes the central core of the house to be cooler than the outer, more distant (from the air-conditioner) parts. The condition is made worse by the effects of summer sunlight, which can heat the southern-exposed side of the home more than the northern side and thus make it even hotter. Once again, equally distributed cool air results in an unequally cooled home, some parts of which are comfortable and some not.

Another factor contributing to this condition is adjacent areas, which may be hotter or colder than the home's living area by design. Even with good insulation in the walls, some heat transfer occurs from the warmer area to the colder one. Exhibit 5-11 shows how outside climate, sunlight, and adjacent areas can all contribute to unequal heating and cooling of a home with only a single zone.

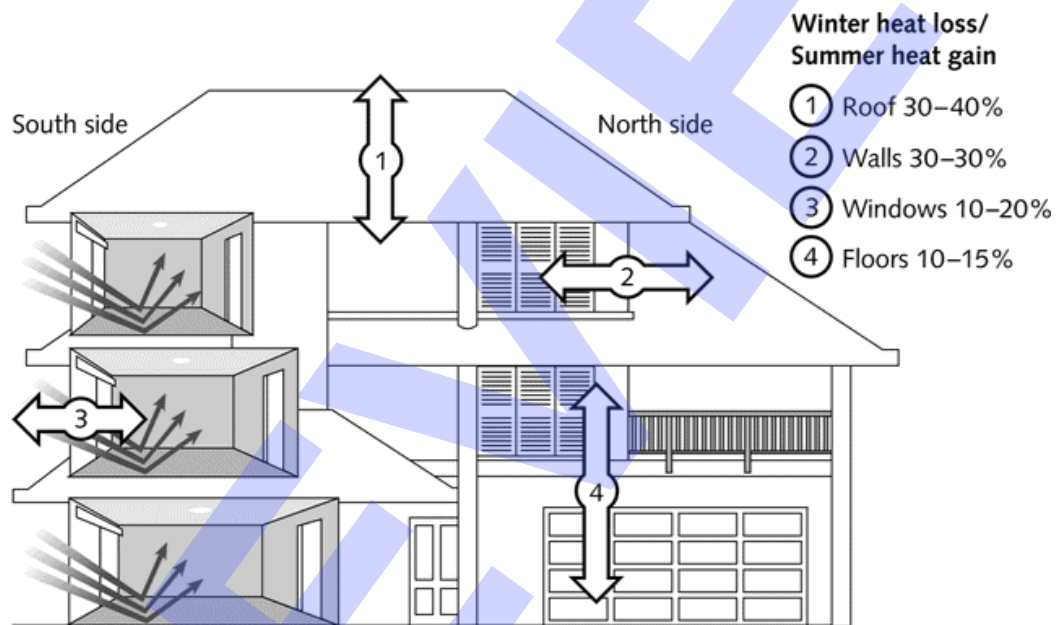


Exhibit 6-6: How heat transfer creates uneven temperatures in a home

Dividing the heating and A/C systems into zones with separate temperature controls in each allows the system to compensate for inequalities in heating and cooling of the home by sending more or less heated or cooled air to needed areas, independent of what's happening in other zones. Each zone is treated as a separate apartment with its own HVAC system and controls. If the controls of each zone had to be continually adjusted for changing conditions by hand, the system would be too cumbersome to use effectively. Automating the HVAC system allows it to be controlled by a preset program based on input from temperature sensors (thermostats) located in each zone.

Master/slave zones

To configure the zones in a master/slave relationship, you can place a thermostat in the zone that will be the master zone. Program this thermostat to function as the master thermostat. In the slave zones connect additional thermostats using RS-232 serial or other communication type connections as required by the thermostats. Program those thermostats to function as slave thermostats. Control signals can be programmed at the master or sent from another control device such as a PC or a microprocessor embedded in another control device.

Ventilators

In addition to heating, some HVAC systems may need to provide for *ventilation*, the exchange of air in the home with outside air. Ventilation may be necessary even when the inside and outside temperatures are the same and no heating or cooling is required. If a home is well insulated and sealed against outside weather conditions, the air inside it remains cut off from outside air unless a door or window is opened. With occupants inside the home, this can result in depletion of the oxygen in the air, stagnant odors, buildup of humidity, and accumulation of dust and bacteria. Ventilation provides fresh air in the home without heating or cooling the new air it brings in. The new air may be filtered or humidified so that it doesn't add to the air-quality problems already present.

For ventilation to be effective, the system must have both an intake vent on the outside of the home, through which outside air is drawn in, and an exhaust vent through which stale inside air is expelled. In a sealed home, an intake vent without an exhaust vent won't work, and neither does the reverse. Both are required. The intake vent may be a part of the HVAC system and controlled so that it can be opened or closed as needed. The outside exhaust vent could also be part of the HVAC system's air return duct system, or it could be a separate vent or vents that exhaust air into the attic, from which it would be expelled outside by an attic fan. Exhibit 5-10 shows a typical A/C system with built-in outside ventilation and exhaust of room air. The amount of outside air entering the system is controlled by dampers (air duct doors).

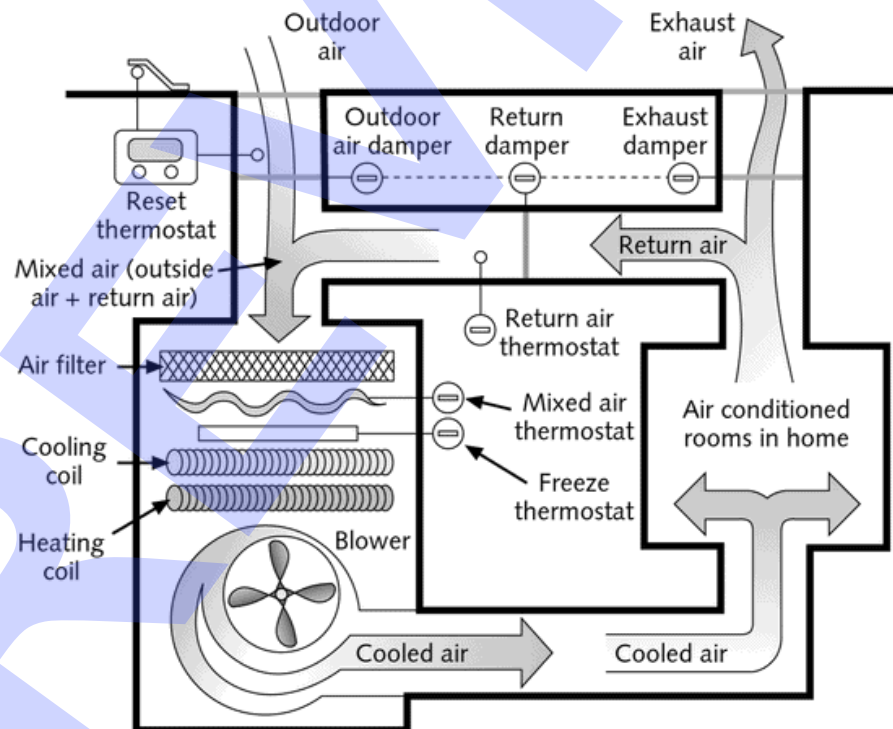


Exhibit 6-7: An air-conditioning system with outside ventilation

Do it!

B-1: Discussing HVAC control

Questions and answers

- 1 What are the four general methods of communication within an HVAC control system?

IP based over CAT5, wireless, serial, and proprietary systems

- 2 What is the purpose of heating zones?

To distribute heat more evenly and efficiently throughout the home.

- 3 About how much heat is lost through the roof in the winter?

30-40%

- 4 What is the purpose of ventilation?

Ventilation provides fresh air in the home without heating or cooling the new air it brings in.

Thermostats

A *thermostat* is the main control sensor used for HVAC systems. It consists of a temperature-sensing device coupled to a switch. A thermostat can be set at a given temperature and, whenever the temperature falls below the set temperature, the switch on the thermostat closes. This sends a signal to the furnace to turn on and raise the room temperature. When the temperature reaches the set level, the thermostat switch opens and this signals the furnace to turn off.

Thermostats can be dual-acting so that they control both heating and cooling equipment. In this case, when the room temperature falls too low and the thermostat switch closes, the furnace turns on. When the temperature is above the set figure and the switch is open, the A/C unit turns on and cools the room until the switch closes, signaling the air-conditioner to turn off. Dual-acting thermostats have a second switch, which sets them to either heat or cool mode. This prevents both the heating and A/C units from being active at the same time. The switch can be set by the user, and it determines which system is operational. Without such a switch, the two systems would conflict with one another, the furnace continually raising the room temperature and the A/C lowering it.

In HVAC systems with multiple zones, a thermostat normally is installed for each zone. This allows the temperature to be set for each zone. The actual temperature set may be the same in each zone, but the individual thermostats are still useful, because they allow the system to act independently in each zone to maintain the desired temperature. Twice as much heat, for example, may be needed to maintain 70 degrees Fahrenheit in a room over an unheated garage on the north side of the house, as is necessary in a sunny room on the south side. The individual thermostats can signal for the necessary heating in each zone.

Controller programming

Once installed, tested, and programmed, a good HVAC control system should function on its own with virtually no required input from the homeowner for long periods of time. Setting and adjusting the system to function on its own may take a little time but results in a comfortable environment over long stretches. This section describes setting the controllers and sensors to operate without additional human input.

Thermostats should be set to a comfortable room temperature, around 68 to 70 degrees in the winter and 75 to 78 degrees in the summer. Some people may prefer only one year-round temperature somewhere in between those given, but most feel better with two settings, and the dual range is more economical as well. Once set, thermostats can be left in the same position indefinitely.

Experience may show that some zone thermostats need to be set a few degrees higher or lower than the desired temperature in order to maintain that actual temperature in the room. This can be a function of the thermostat itself (it reads slightly above or below the actual temperature) or its location (it's placed in the room where the temperature is consistently higher or lower than the room average). There's nothing wrong with making these adjustments, and they won't affect the economy of the system as long as the actual room temperature level (as contrasted with the thermostat setting) isn't increased substantially.

Zone programming

The control panel, based on input from the thermostats, starts the HVAC system (furnace or A/C), as needed, and opens or closes the dampers to each zone, as required. Only those areas of the home that need heat or cooling receive it. In radiant systems, the controller opens or closes the appropriate valves on the piping system to control the flow of hot water.

Zones can be set to maintain different temperatures if desired. A garage or storage room, for example, might be kept 10 or 15 degrees colder than the rest of the home. The garage might be eliminated entirely from the A/C system. A sunroom might be allowed to rise 10 degrees above the rest of the home's A/C level and, in winter, to drop 10 degrees below the heated level of other rooms

Time-of-day programming

Many people prefer lower heating temperatures at night, and a control panel or programmable thermostat in a single-zone HVAC system usually permits such time-of-day changes. The typical system allows for four temperature changes per day, so a day's program might look like this:

- 5:30 a.m. — Temperature up to 70 degrees prior to family awakening.
- 8:00 a.m. — Temperature down to 55 degrees while family is at work or school.
- 4:30 p.m. — Temperature up to 70 degrees prior to family's arrival home.
- 10:30 p.m. — Temperature down to 65 degrees while family is asleep.

Weekend times and temperatures would probably be adjusted somewhat differently, because the family's schedule would be different on those days. Exhibit 6-8 shows an automated thermostat for a single-zone HVAC system. A control panel has similar inputs for a zoned system.



Exhibit 6-8: An automated thermostat control.

Seasonal presets

In addition to timed temperature settings on a daily basis, control panels allow for longer-range settings as well. These seasonal adjustments can include temperature changes that vary depending on the time of year and time adjustments for away periods. If the home isn't occupied year-round, the HVAC system can be programmed to reduce operation to the minimum needed to avoid freezing or overheating whenever the occupants aren't in the home. This can be programmed automatically (using a motion sensor and a time delay: if no motion is detected in the home for 12 hours, the minimum operation cycle starts) or it can be integrated with the home's security system (whenever the security system is armed because the family is away from the home, the HVAC system goes to minimum operation status)

Remote access

The minimal operation function of an HVAC system, whether timed or activated by a security system or sensor, is made better by a remote access feature for the system. Since no one likes coming home to a cold or overheated house, being able to contact the HVAC system by telephone or by computer on the Internet enables the homeowner to call ahead so that the home temperature is normal when the family arrives. When the owners are away, the HVAC system is on minimum operation. When they arrive at the airport an hour away from the home, a telephone call and a few command inputs changes the home's HVAC system to normal operation so that, by the time the owners arrive at the front door, the home is heated normally and ready to receive them

Do it!

B-2: Programming thermostats

The thermostat can be programmed without being connected to an HVAC system.

Check the documentation for the thermostat for the steps to set the Day of week.

Check the documentation for the thermostat for the steps to set the hours and minutes as well as the AM or PM setting.

Here's how	Here's why
1 Install a battery in the automatic thermostat	You'll program four time-of-day settings with corresponding temperatures into an automatic thermostat.
2 Set the Heat/Cool switch to Heat Set the master switch to ON	
3 Set the Day to <i>today</i>	If necessary. Where today is the day of week. Most thermostats have a Set Day button or some similarly labeled button and begin with Monday as 1 and end with Sunday as 7.
4 Set the time to the current time	Most thermostats have a Set Clock button or some similarly labeled button. Be sure to set a.m. or p.m. as needed.
5 Press the button to begin programming	A button labeled View Program or Program or some similarly labeled button is used on most thermostats.
6 Set the first programmed time to 5:30 a.m. Set the temperature to 70 degrees Fahrenheit	
7 Press the button to begin programming the next setting	
8 Set the second programmed time to 8 a.m. Set the temperature to 55 degrees Fahrenheit	
9 Press the button to begin programming the next setting	
10 Set the third programmed time to 4:30 p.m. Set the temperature to 70 degrees Fahrenheit	
11 Press the button to begin programming the next setting	

12 Set the fourth programmed time to 10:30 p.m.

Set the temperature to 60 degrees Fahrenheit

13 Press the button to run the program

Most thermostats have a button labeled Run Program or some similar wording.

Topic C: Lighting control

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
5.5	Describe basic lighting terminology and install peripheral control devices. <ul style="list-style-type: none"> Identify lighting control applications <ul style="list-style-type: none"> Indoor and outdoor Centralized and distributed Dimming Scenes Relay/switching Occupancy/motion sensing Communication interface/bridge <ul style="list-style-type: none"> Power line phase couplers Identify lighting control protocols <ul style="list-style-type: none"> Z-Wave Zigbee PowerLine Carrier (X10 protocol/PLC) UPB (Universal Powerline Bus) Proprietary RF and proprietary low voltage <ul style="list-style-type: none"> Recognize compatibility issues Time and event driven Window treatments Energy management Security interface Lighting connectivity Motor speed control

Lighting control applications

Explanation



Lighting control applications include both the types of areas and types of interface you will be using. These can be locally or centrally controlled.

Indoor and outdoor

Both style and design are different for indoor and outdoor applications. Outdoor fixtures and controllers must be robust enough to withstand weather extremes without failing or creating a dangerous electrical fault if the unit's seal leaks.

Centralized and distributed

A centralized approach to controlling the lighting for a home or building works well when the use of the home or building is occupied on a regular schedule. You can configure the central control panel to turn off the lights at a preset time and turn them on again at a preset time.

Some whole house control systems enable you to turn off all the lights from a single master switch. If you have the system connected to a PC, you can create macros that turn the lights on and off on a regular schedule. Some even let you bring them on based on dusk/dawn settings.

In a distributed system, lights are controlled separately rather than from a central location. The typical light switch in a room is an example of a distributed lighting method. You can also configure lights to come on when a room is occupied. When no activity or human presence is detected after a certain period of time, the lights will automatically turn off.

Dimming

Dimming modules that can dim a single room light or several lights wired together are now common in automated homes. Manual dimming modules can be incorporated into any wall switch and used to control the lights connected to the switch. These modules can be controlled with X10, ZigBee, or Z-Wave technology in order to automate the lighting system completely. Wireless lighting controls can be connected to the home LAN through an Ethernet-compatible device. We'll discuss automated home lighting controls later, but any needed additional or upgraded AC wiring should be in place before the automation is installed. X10 controlled dimmer modules can be manually operated from the switch. They can be installed and used before the automated system is activated.

Dimmer modules are wired in the same manner as regular switches and can be configured as single-pole switches, single-pole, double-throw switches, or double-pole, double-throw switches, without affecting the dimming component.

Scenes

A *lighting scene* might consist of the lights in a single zone, but can also be any set of lights designed to accomplish a specific lighting objective. A dining scene, for example, might dim the overhead dining room chandelier while turning on small spotlights to illuminate the paintings on the room's walls. Another lighting scene in a family room might dim the overhead lights to eliminate reflections on the glass while turning on backlighting behind the aquarium to make observation of its occupants easy. Still a third scene might turn off floodlights in the back yard garden while illuminating the flowers, fountain, and footpaths with indirect lighting for a romantic effect.

Occupancy/motion sensing

An occupancy sensor is basically a motion sensor that turns off the lights when there is no one in the room. It uses motion or IR detectors to determine if anyone is in the room.

Relay/switching

Switches are installed in circuits to control lights or outlets. They can be wired in several configurations, but the most common is as a single switch controlling a light or outlet, as shown in Exhibit 6-9 option a. Another wiring configuration is shown in Exhibit 6-9 option b. It shows how two switches can control a single device such as a light fixture or outlet. This allows convenient access from opposite sides of a room, the top or bottom of a stairway, or the inside or outside of the home. This arrangement uses double-pole, double-throw switches and is known as a three-way switch.

A third configuration, shown in Exhibit 6-9 option c, also provides for a three-way switch, but gives one of them ultimate control (either on or off). With this arrangement, switch 1 can turn the light on and it remains on regardless of the position of switch 2. If switch 1 is in the off position, switch 2 can turn the light on or off, but only so long as switch 1 remains in the off position. This last configuration is more useful in an automated system than with a strictly manual one.

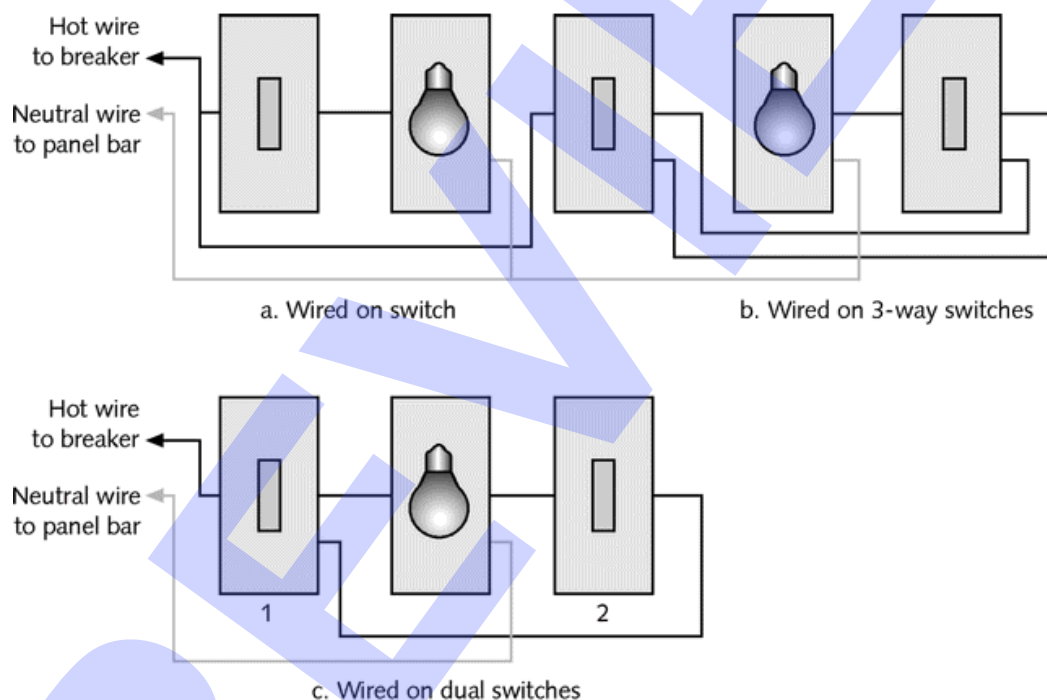


Exhibit 6-9: Options for wiring switches

Time and event driven

A control system that can bring the lights on in response to an event can be very useful. They might be triggered by the door being unlocked, by a motion detector sensing movement, by a door/window sensor being opened, or any other of a myriad of events.

You can also configure a system so that lights come on and go off at preset times. You can configure them to come on or off in response to sensing the arrival of dusk and dawn as well.

Window treatments

Window shade control mechanisms are available with X10 technology. While not really lighting controls, these modules can be very useful in controlling sunlight through windows, darkening entertainment centers in daylight hours, and other related functions. X10 control modules connected to motorized pulls can open shades, blinds, or curtains, close them, or partially open or close them.

Manual remote-operated window coverings are mostly used where the windows are high and inaccessible for hand pulls. An automated shade or curtain system can be programmed like a lighting system to respond to time-of-day commands, sunrise and sunset macros, or other command sets.

Energy management

An energy management system helps reduce energy consumption, by timing or sensing when lighting needs to be on. The national energy code standard, ASHRAE/IES 90.1-1999, requires that lighting systems automatically shut-off in buildings over 5,000 square feet. Critical loads that must be operated continuously are not bound by this requirement.

Security interface

Even in a lighting system that is controlled to turn off and on at certain times or under certain conditions, you can have the lights turn on as part of your security system. If an intruder triggers an event, you can link the trigger to turning on the lights. Most intruders will not be willing to stay in a home with all of the lights suddenly turned on.

Lighting connectivity

An automated home lighting system, whether it's wired or wireless, won't add any load to the home's AC electric wiring, but the adequacy of the in-house wiring should still be confirmed before installing any automation. Both wired and wireless automation controls are subject to interference or "noise," which can be caused or increased by overloaded wiring.

Lights are usually not the cause of *overloading* in a home electric system, because they aren't the largest consumers of electricity in the system when they're used individually. If acting as a group, such as when an automation system turns on or off all the controlled lights in a home simultaneously, lights can have a significant impact on the power system. However, individual lights being turned on or dimmed won't make much of a difference in the overall power consumption or load. Unlike electric motors, which draw heavy current when starting, lights consume only slightly more electricity when starting than they do when operating and a decline in line voltage won't cause a light to consume more power either. If line voltage drops, the light simply shines less brightly; that's how dimmers work.

Before installing home lighting controls, determine if a home's wiring is adequate. If new circuits, wiring, or fixtures are needed, they should be installed before the automation or at the same time. New circuits, if necessary, can be used not only to reduce the load on older wiring but also to connect additional new lighting that might not have been installed at all if the new circuits weren't available. Automation devices like controlled outlets and switches can be installed in new circuits at the beginning, instead of replacing manual units, as is necessary in existing circuits.

All these considerations point to the need for a plan for the lighting system itself and for the automation system that controls it. The plan should start with a map of the existing electrical system. Make the diagram of existing wiring as complete and accurate as possible on a floor plan of the home. Add any new circuits that are required and design how the wiring for these will be installed. Finally, design the control system, noting exactly which lights you plan to control, which lights will be controlled as *zones* (groups of lights controlled as single units), and where the controllers will be located. Make the plan as detailed and complete as you can. Every item planned before starting the hands-on work enables you to avoid problems during the installation phase.

Label the plan with a unique label for each item. As you later install each device, it should be marked with the label you gave it in your plan. The plan can then serve as a schematic drawing of the completed lighting automation system, which you can use in the future to troubleshoot and maintain it. Exhibit 6-10 shows a plan of the first floor of a large home with all the electrical fixtures noted. Because the plan has been reduced in size for publication in this book, the fixture symbols have been enlarged and only those in the family room are shown labeled.

All the high-voltage fixtures in the home should be grounded, as should those installed with any new circuits added as part of the automation remodeling. Non-grounded fixtures are almost never found, except in old homes constructed before grounding was a code requirement. As a safety measure and also because any ungrounded circuit is likely to cause interference in the automation system you install, it's still wise to check that everything is, in fact, grounded. This is true whether it's a wireless system or uses *power-line technology*. *Fluorescent lighting* is especially prone to generate interference in the automated lighting system, as well as in other home technology installations.

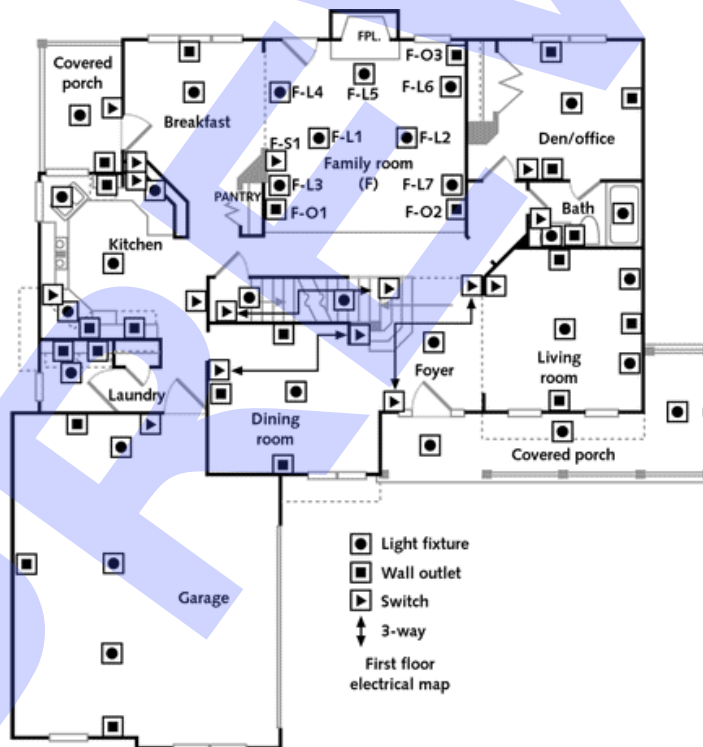


Exhibit 6-10: Electrical fixtures noted on floor plan with those in one room labeled



When a light is connected directly to its power supply, it's said to have a *home run connection*. A lamp plugged into an outlet receptacle is an example of a home run-wired light, as is an overhead light connected to a switch on the wall. The light is wired directly to a power connection (a home run wire) inside the walls. Most, but not all, hard-wired lights (those that are wired as part of the home's electrical system) are home run lights. They're connected to the electrical system through a switch, which allows them to be turned on and off.

Sometimes a switch controls two or more lights. In this case, not all the lights may be wired to the electrical system directly through the switch. One light may be wired to the switch and the second light connected to the first light, getting its power from the first light's connection to the electrical system (if there's a third light, it would be connected to the second light). This arrangement of connection is known as *daisy chain wiring* (from the now little-known art of joining daisies by twisting the stem of one around the blossom of the next). Other examples of daisy chain electrical connections are as follows: a series of lamps in which the first is plugged into a wall outlet, the second is plugged into a connection in the first, and perhaps a third into a connection in the second; or a television that's plugged into a wall outlet and a small backlight lamp is connected to the television. Exhibit 6-11 shows two lamps with home run connections on the left and three lamps connected in a daisy chain on the right.

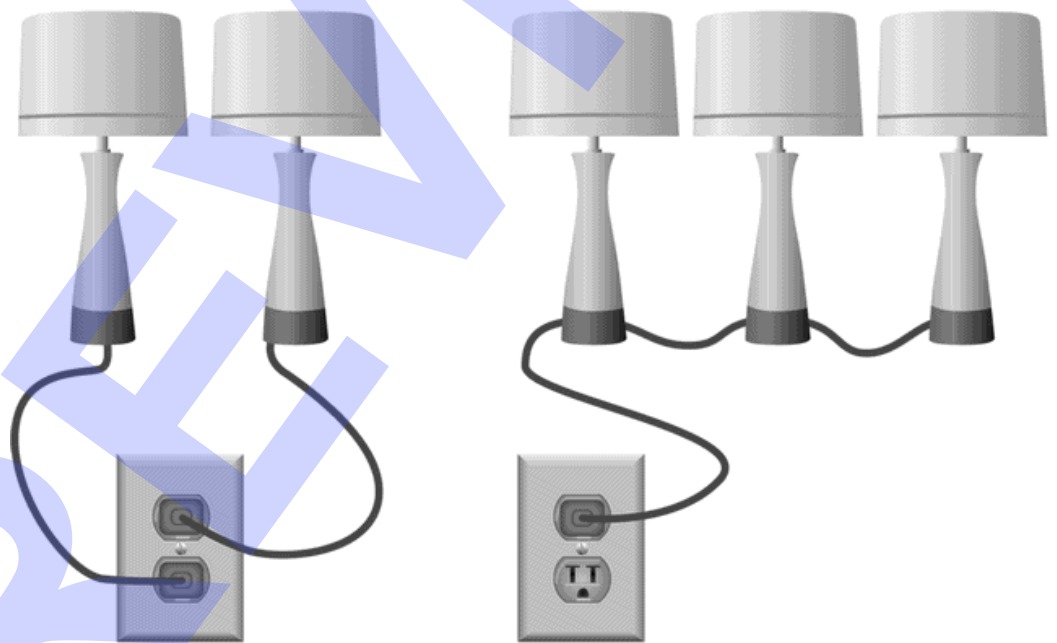


Exhibit 6-11: Lamps with home run connections (left) and daisy chain connections (right)

Lights with daisy chain connections always work together from a single control device, because all the lights in the chain receive their power from one connection. They're wired in parallel, however, not in series, so that if any one light fails, the others in the chain continue to work. Daisy-chained lights are useful, because the arrangement permits several lights to be placed in one location without using all the wall outlets. Multiple track lights and indirect fluorescent lights are often connected in daisy chains. Decorative lighting, both indoor and outdoor, is usually in a daisy chain in multiple light segments. Parallel-wired holiday lights are daisy chains, and several strings of them can be connected, one to another, in an even larger chain.

Only one control device can be used on an entire daisy chain, however, because it's all powered from only one controllable point.

Home run-connected lights that are part of the home's electrical system can be controlled individually from the switch that's always wired into their circuit. They can also be controlled from another switch wired into the circuit closer to the light than the first switch, if the first switch is left in the on position. Home run lights plugged into a wall outlet can also be controlled at the outlet or by another switch wired into the light's cord. Because each home run light has its own power connection, it must be controlled by a separate controller. Most plug-in controllers have two or more outlet connections, but all of these are usually controlled by the same commands, and so all the lights plugged into the module work together as if they were one. Exhibit 6-12 shows two lights added in one corner of an under-lighted room (a matching pair was placed in the adjacent corner). These lights connect to a wall outlet and have no manual switch on their circuit. They can be controlled, however, by a control module plugged into the outlet and commanded by a controller.



Exhibit 6-12: Added lights controlled by an automated system

Motor speed control

Ceiling fans should never be controlled by a dimmer switch. However, using a motor speed control device enables you to provide the functionality of a dimmer switch. It uses pulse width modulation to adjust the speed of the current going to the light or the ceiling fan.

Do it!

C-1: Programming lights to turn on when motion is detected

Here's how	Here's why
<div>1 Set up a lamp connected to a lamp module</div> <div>Turn it off</div>	<div>You'll set up and test a basic light control system consisting of a motion sensor and two control modules, each controlling a light.</div> <div>Leave the lamp's switch on and use a remote control or Active Home to turn off the lamp.</div>
<div>2 Set up a motion sensor at least 6 feet off the ground in one corner of the room</div> <div>3 Arm the security console</div>	
<div>4 Wait at least a minute without moving, then walk in front of the sensor</div>	<div>The lamp should come on when the motion sensor detects movement.</div>

Lighting communication interface/bridge

Explanation



Digital Addressable Lighting Interface (DALI) is a protocol that defines how digital light ballasts perform. Each DALI device is individually addressable. The devices can operate with any device or controller that is DALI compliant. The DALI compatible lights can be centrally controlled or controlled. For example, you could dim all of the lights throughout the house at once using a DALI compliant system. Then, you could bring up the brightness in an individual room using a local control such as a regular light switch. Up to 64 digital ballasts can be connected on the network.

More information about DALI can be found at www.buildings.com/Articles/detail.asp?ArticleID=1870.

An interface/bridge connects a DALI interface to a standard computer port. The interface/bridge translates signal levels and protocol between computer ports and DALI signal levels and protocol, and back again. An integrated circuit chip is used for translation and buffering. Signal level translation also monitors the voltage levels of the DALI bus.

Power line phase couplers

Home automation systems transmit their signals at specific points during the alternating current electrical signal. When two systems are connected that are out of phase, signals cannot be transmitted across the junction or the signal quality is degraded. A power line phase coupler attaches to both sides of the connection point and transmits the signal between them.

Such a phase coupling problem is typically solved by installing a device in your home's electrical panel. Without such a device, your automation signals must travel out of the house to the transformer (typically mounted on a nearby telephone pole) and then back into the house. With the power line phase coupler, the signal can cross phases while remaining within your house's wiring. This improves the signal quality and strength.

A power line phase coupler is used for sending data signals between power line phases. The power line phase coupler system includes a female and a male connector which is electrically connected to the female connector by a length of cord. It also contains a repeater coupler. The repeater coupler is electrically connected between Phase A and Phase B of the male connector for repeating and amplifying a data signal received from the communication interface bridge.

Lighting control protocols



The home control protocols that you examined earlier are often used to control lighting. In fact, many of them were originally designed as lighting control methods. They later were expanded to include control of other devices. The lighting control protocols include:

- Z-Wave
- ZigBee
- X10
- UPB

Z-Wave

Z-Wave is a wireless home control protocol based on the Z-Wave standard. This standard works at 908.42 MHz in the United States. In Europe it operates at 868.42 MHz. It has a range of approximately 100 feet. It routes signals from one device to the next, making the network as large as you need it—there is no distance limit due to the routing from device to device. You can control up to 192 devices using this protocol.

It enables you to control lamps and light switches as well as outdoor lights. You can turn all of the lights off or on with a single button. It also has the ability to be programmed for lighting scenes in which you can dim or brighten the lights.

ZigBee

ZigBee is a wireless control protocol intended for use in applications with low data rates and low power consumption. This includes not only home applications such as smoke detectors, security systems and building automation, but also industrial control, embedded sensing, and medical data collection. Devices on a ZigBee network use very small amounts of power so individual devices often run for a year or more without needing to change the battery. ZigBee operates in the industrial, scientific and medical radio bands; 868 MHz in Europe, 915 MHz in the United States, and 2.4 GHz in most jurisdictions worldwide.

Up to 64,000 nodes can be controlled from a single master device. This protocol has fast response times, which makes it a good choice for controlling lighting. Users expect pressing a light switch to immediately turn on the light, so ZigBee is able to address this requirement.

PowerLine Carriers

Some control protocols use the existing wiring in the home as the structure for the control network. This is known as a PowerLine Carrier or a PowerLine Communications network. Examples of this are X10 and the HomePlug product lines.

X10 products use either a standalone controller or your PC to control devices. The devices include things such as lights and appliances, the ability to broadcast photos and PC-based music to an entertainment center, or to monitor an important area of the home or business.

The HomePlug Alliance, an industry group established by companies that manufacture products for the power-line networking technology, has selected a newer technology called PowerPacket as the standard for power-line networking. Intellon developed this technology, and several companies are now producing products based on it.

Power-line networks offer many of the same advantages of HomePNA networks because both use existing wiring rather than requiring new installation. Among the features that power-line technologies offer are the following:

- The system can be installed one unit at a time wherever an electric outlet is available.
- Power-line networks can accommodate both PCs and Macs.
- Power-line networks function as peer-to-peer systems, which require no hubs or routers. All data is sent to all nodes. Each node reads only what is addressed to it and discards the rest.
- Power-line technology transmits data at frequencies that don't interfere with the low-frequency AC electric current flowing in the same wire. The network can function without regard to whether electric current is flowing or how much.
- Power-line technology allows data transmission at rates up to 14 Mbps, which is easily able to meet all home network requirements.

UPB is a competing technology to the popular X10 control system.

UPB

Universal Powerline Bus (UPB) is a control system that uses the existing AC wiring within your home to carry control signals. UPB uses low frequency, spread spectrum transmissions that are resistant to noise and degradation. Each UPB component is assigned a Network ID. When control signals are sent out part of the signal is the Network ID. Only devices that have that specific Network ID will respond to the signal.

UPB manufacturers claim that their technology is more reliable, faster, and more scalable than X10 or other technologies. For example, one manufacturer claims that their UPB systems can manage over 62,000 “loads” (devices) per system compared to X10’s limit of 256 and can send five commands per second compared to X10’s one.

Proprietary RF and proprietary low voltage

Any proprietary system of control is specific to the manufacturer of the control units. They may offer advantages not available from the standardized protocols. However, only devices from that manufacturer work with the system, limiting your choices for future purchases.

Compatibility issues

The disadvantage of a proprietary system is that it is manufacturer specific. This results in it possible being unable to interface with standardized components. Also they are subject to the whims of the manufacturer for future compatibility and availability.

Some of the technologies, be they proprietary or standardized, do not work well when they are installed with another technology. The signals cross between the two systems with unpredictable results. Other technologies, for example UPB and X10, can peacefully co-exist in the same house without any interference between the two systems.

*Do it!***C-2: Installing lighting control devices**

Here's how	Here's why
1 In ActiveHome Pro, right-click Room#	You will install an X10 based dimmer switch and control it through ActiveHome Pro software.
Choose Add Module	
2 Name the new module Dimmer#	Where # is your lab number.
3 From the Type of Module drop down list, select Lamps	To match the lamp module.
From the Module drop down list select Decorator Style Wall Switch Module	
Set the House Code and Unit Code	
Click OK	To turn on the lamp.
4 Click the light switch icon	
5 Drag the slider to the mid-point	The slider is next to the light switch icon and adjusts the intensity of the lamp's bulb.
6 Using an X10 remote control, press the off button	This is the Channel down button.
Press the on button	This is the Channel up button.
Press the dim button	This is the Volume down button.

Topic D: Power protection

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
5.6	Identify and install component power protection devices. <ul style="list-style-type: none">• Identify whole house protection options<ul style="list-style-type: none">• Surge suppression• Power conditioning• Identify and install point protection<ul style="list-style-type: none">• Surge protectors (high voltage and ancillary low voltage devices)• UPS (Uninterruptible Power Supply)• Power conditioning

Whole house protection options

Explanation

Power conditioning is the process of restoring a problematic AC signal to a high-quality smooth signal that is safe for your computer and other electronic devices. Power conditioning equipment includes surge protectors, battery backup devices, and generators.

Surges and spikes

An electrical surge is a sudden momentary increase in the rate of current flow or the voltage in a circuit. Surges can be produced by power equipment starting up or shutting down either inside the home or at a more distant location, or by lightning strikes or other atmospheric electrical disturbances. Another name for a power surge is a spike, although some people define a spike as having a shorter duration and a higher voltage than a surge.

Both surges and spikes mean that for a short period of time there is too much electricity in a circuit. These electrical excesses may last only a few millionths of a second or they may persist for many times that long. In either case, they can do serious damage to electronic equipment.

The electric potential forced into the circuit by a surge may discharge by arcing from wiring to a ground connection. The heat of such an arc can fuse components or burn them out just as a light bulb filament shatters when subjected to excess power. Even relatively small surges, repeated over time, reduce the life of low-voltage electronic parts by subjecting them to momentary current flow and resulting heat far above their designed maximums.

Surge suppression

Devices are available to protect against surges and spikes. These can be installed at the point where network devices connect to the AC power or at the point where potential carriers of *surges*, such as AC power lines, telephone lines, and television cables, enter the home. Because surges can originate from within a home or from outside, protection from both sources is necessary to prevent damage to home electronic equipment. This dual protection is particularly important when part or all of the network's data transmission wiring is shared with or connected to television cables, telephone lines, or outside antennae.

Surge suppressors that can be installed at electric outlets vary widely in price and quality. The primary consideration for a surge protector is how fast it acts when a surge occurs. If suppression starts only after 0.1 seconds of increased voltage, for example, most surges will have come and gone, doing whatever damage they're capable of, before the suppressor even begins to respond. Such devices are useless for protecting against surge damage.

Devices that can suppress only a few thousand surge amps are also useless. The most damaging surges often attain up to 50,000 surge amps for a few millionths of a second, during which time they can burn through low-capacity suppressors and wreak havoc among low-voltage electronic circuits.

Home LAN equipment should be protected by grounded surge suppressors that are rated to act within a few picoseconds and suppress at least 50,000 surge amps. These industrial-grade suppressors are available in the same one, two, four, and six socket configurations as the less effective "power strip" models, and they look much alike. The high-quality units can be distinguished by two factors: they have their response time and suppression strength ratings printed on them (low-rated suppressors rarely publish their numbers), and they cost more than unrated units. Expect to pay between \$50 and \$100 each for these suppressors, depending on their configuration and amperage.

Combination surge suppressors and noise filters are available for installation on telephone lines, cable television lines, and satellite antenna lines. In all cases these suppressors should be placed in the lines before they connect to any network equipment. The vast majority of their effect on the home network is improved performance from noise and interference reduction, but the few times they intercept a surge or spike prevent far more damage than their cost, which is about the same per unit as a good AC suppressor.

Surge protection on the main AC power lines coming into the home usually takes the form of a circuit interrupter that cuts off the electric current when the voltage rises above a preset maximum or drops below a preset minimum. Either condition can damage electric equipment, although electronics are more vulnerable to high voltage than low. Electric motors, such as those on furnace fans, air-conditioning compressors, refrigerators, and freezers, can overheat and burn out if the voltage drops too low over a period of time.

Main line interrupters are expensive and are probably only warranted in areas where the danger of surges originating outside the home is fairly high. A little research into the weather history of a location and a check of whether any large-capacity commercial or industrial electrical equipment is operating nearby can help determine whether a power line interrupter should be installed in a home system. A middle course of protection may be to install smaller interrupters on individual circuits that power expensive equipment.

*Do it!***D-1: Identifying whole house protection options**

Here's how	Here's why
1 Using a search engine in a Web browser, search for whole house power options	You will identify whole house power options and determine how large of a unit you would require.
2 Determine the available power provided by the generator	
3 Determine if it would be large enough to power the main electrical components in an average home	You can search the Web for a site that lists typical wattages of common household appliances and electrical subsystems.
4 Determine what additional features are available or required to make the system work	
5 Compare your results with your classmates' results	

Identify and install point protection

Explanation

Point protection for critical loads is accomplished by small, individual power conditioners. These should include filtering, surge suppression, and isolation.

Surge protectors (high voltage and ancillary low voltage devices)

Surge protectors are the most basic point protection that should be employed. They will not supply power in a blackout situation but will stop dangerous voltage spikes from destroying electronics.

High voltage surges can be caused by external sources such as lightning strikes, animals in contact with power line equipment, or as the result of utility pole accidents. These surges might enter the home via electric or telephone lines. Surges can also occur when large appliances within your home such as air conditioners and refrigerators turn on or off. The surges can damage computers, network equipment, and other electronic devices.

Low voltage circuits are those that operate at 115 volts. These circuits and the devices connected to them also need protection from surges. Ancillary low voltage transistors are part of some integrated circuits and can easily be damaged by electrical surges.

UPS

Many home security systems have backup battery power, which can be used in case of power failure, or some type of failsafe system that warns if power is low or sends an emergency signal in the event of power failure. This backup power method is sufficient for most systems, but if the home network has an *uninterruptible power supply (UPS)* for use in maintaining all or part of the LAN's operational ability during a power failure, this power backup can easily be configured to include the home security system. Security panels don't require a lot of power and so won't put a heavy drain on a UPS designed to supply and protect the network.

A 12- or 24-volt security panel powered by an AC adaptor can simply be plugged into one of the UPS outlets, and the unit is supplied through the UPS. Wired sensors that are powered from the security panel are also powered by the UPS through the adaptor hookup. Wireless devices that are battery-powered can't be connected to a UPS, but they also aren't affected by a power failure and shouldn't need backup power. Their low-battery warnings should always be heeded so that they don't lose battery power in an emergency situation.

Home UPS systems are battery-powered and have limited operating times under load. They're not designed to keep large systems running, only to give enough time for orderly shutdown so that no data is lost. The home security system won't tax a UPS nearly as much as the LAN will, but when other devices deplete the UPS batteries, the security system shuts down as well. In the event of power failure, the operating limits of the UPS should be noted and the homeowner should be aware that the security system ceases functioning when the battery power runs low.

Power conditioning

A *power conditioner* is an electronic device that smoothes out the peaks and dips of household AC power. This is also known as a line conditioner. They create smooth power for precision electronics, such as computers and sound equipment. Many power conditioners also function as surge protectors.

Power conditioners differ from the typical uninterruptible power supply because they continuously charge the battery and continuously run the equipment off battery power. Most UPSs pass the source power straight through while the household power is on. This may cause some equipment to fault or perhaps even be damaged in a brownout or spike current. Using a power conditioner when running an electric generator for electronics is a good idea. It will help even out the power and help prevent damage to electronic devices running on generator power.

Do it!

D-2: Installing power point protection

Here's how	Here's why
1 How much protection does a surge protector offer?	<i>The devices connected to it will be protected from spikes and surges. However, your devices will still be susceptible to brownouts, blackouts, and noise.</i>
2 What types of systems should be protected by a UPS?	<i>Given that UPSs are available for as little as \$40, most computers should be protected by a UPS. You might also consider protecting TVs, stereos, and other home electronics with a UPS.</i>
3 Connect a lamp to the power conditioning equipment provided by your instructor	Your instructor will provide surge protectors or UPSs for you to install.
4 If you installed a UPS, unplug the UPS from the wall	To simulate a blackout condition. The lamp should stay lit.

Provide students with a mix of surge protectors and UPSs.

Unit summary: Home control and management

Topic A

In this topic, you identified methods used to integrate control subsystems. First, you examined **embedded control systems**. Next, you installed a **PC-based control system** and identified various **user interface devices**. You also looked at various communication protocols used to communicate between subsystems and control devices including **IR, RF, Bluetooth, serial, IP, and contact closure**. In addition, you examined **ZigBee, Z-Wave, and proprietary protocols** as well as the use of **ASCII** to send messages.

Topic B

In this topic, you described basic **HVAC** terminology and installed peripheral control devices. You learned about the **control and communication layers** involved in HVAC control, and examined compatibility issues. You also learned that communication could be done over **IP, wireless, serial, or proprietary protocols**. Next, you examined **HVAC zones** including the **master-slave** and **microprocessor controlled** configurations. Finally, you examined how to **program a thermostat**.

Topic C

In this topic, you described basic **lighting terminology** and installed **peripheral control devices**. First, you learned about the **lighting control applications** including indoor/outdoor, centralized/distributed, dimming, scenes, relay/switching, occupancy/motion sensing, time/event driven, window treatments, energy management, security interface, lighting connectivity, and motor speed control. Next, you examined the **communication interface/bridge** and **power line phase couplers**. Finally, you examined lighting control protocols including **Z-Wave, ZigBee, X10/PLC, and UPB**, as well as **proprietary methods** and compatibility issues.

Topic D

In this topic, you identified and installed component **power protection devices**. You examined both **whole house protection** systems and **point protection** systems. You learned about **surge suppression, UPSs, and power conditioning**.

Review questions

- 1 Another name for an embedded control system that is built into the device it controls is _____.

firmware

- 2 List some of the user interfaces that can be used with control systems.

Remote controls, keypads, touch screens, keyfobs, telephones, SmartPhones, cell phones, PDAs, Web tablets, PCs, and laptops

- 3 What is the most popular form of IR wireless?

ISDL

- 4 Bluetooth devices connect via a _____.

piconet

- 5 List two factors that make zones necessary in many home HVAC systems.

Distances from the central furnace to some parts of the home and the effects of outside climate

- 6 A thermostat is the main _____ sensor used for HVAC systems.

control

7 Zones can be set to maintain different temperatures if desired. True or false?

True

8 A light connected directly to its power supply is considered to have a _____ connection.

home run

9 An interface/bridge connects a _____ interface to a standard computer port.

Digital Addressable Lighting Interface (DALI)

10 What is an electrical surge?

An electrical surge is a sudden momentary increase in the rate of current flow or the voltage in a circuit.

Independent practice activity

- 1 Design a zoned HVAC system for a two-story, 3,000 square foot home.
- 2 Using the Internet, locate a programmable thermostat to function in the master/slave relationship for the heating/cooling zones.
- 3 Compare the costs of control interfaces and devices for Zibgee, Z-Wave, and RF systems.

Unit 7

Troubleshooting DHTI systems

Unit time: 120 minutes

Complete this unit, and you'll know how to:

- A** Identify and apply the fundamentals of troubleshooting and diagnostics.
- B** Troubleshoot common wireless interference issues.
- C** Apply troubleshooting skills to integrated subsystems.

Topic A: DHTI troubleshooting and diagnostics

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
6.1	Identify and apply the fundamentals of troubleshooting and diagnostics. <ul style="list-style-type: none"> Use of testing equipment <ul style="list-style-type: none"> Multimeter Cable tester Refer to prior documentation Demonstrate when to communicate with technical support and what information is relevant Identify demarcation and responsibilities of associated trades and utilities

Multimeters

Explanation

A meter that can measure multiple electrical properties is called a *multimeter*. Multimeters are available in digital and analog models. Digital multimeters output discrete numeric values on an LED or LCD display. Analog multimeters, the older type, display their output using a needle and dial.



Exhibit 7-1: A digital multimeter



Exhibit 7-2: An analog multimeter

Using a multimeter

Before taking a measurement with a multimeter, you must set options with a dial, button, or other means to indicate what you're about to measure. For example, if you were using a meter like the one shown in Exhibit 7-1, you would press the appropriate buttons to indicate which electrical property you were going to read.

Measuring resistance

To measure *resistance*, first turn off the device you're measuring and disconnect it from its power source. You can damage your meter if you leave the device connected to the power source.

Additionally, you might need to disconnect the device from its circuit. If it remains connected and multiple paths through the circuit exist, you will get misleadingly low readings.

Set the multimeter to read resistance. On some meters, you must indicate the resistance range you expect to be reading. Touch the black and red probes to either side of the circuit to be measured, and read the resistance from the meter's display.

If you're using an analog meter and the needle moves very little or moves all the way to its maximum, you will need to choose another resistance scale.

Measuring voltage

To measure *voltage*, set your multimeter to read either DC or AC voltage. On some meters, you must also indicate the voltage range you expect to be reading. Next, you touch the black probe to the ground and touch the red probe to the spot where you want to measure the voltage.

If you're using an analog meter, the needle might try to swing backward. This indicates that you have the red probe on the ground. Reverse your contact points to take the reading.

The device must be connected to its power source while you measure voltage. The device might need to be turned on, too.

Measuring current

To measure *current*, you must break the circuit and insert the meter in the break. The current in the circuit will then flow through the meter, which by design should offer little disruption and not change the reading appreciably.

A device specifically made for measuring current is called an *ammeter*. A special form of ammeter, called a clamp ammeter, clamps around a wire to measure the current flow. Such a meter does not require you to break the circuit. Clamp ammeters are often used by electricians to measure current flow in 110 V and higher circuits.

Measuring continuity

You can determine if a fuse is good or a wire is whole by measuring continuity. You might also use this technique to determine which pins on one end of a cable are connected to which pins on the other end.

To measure continuity, you can set your multimeter to display resistance (ohms) and look for circuits with zero resistance. Or, if your multimeter includes a continuity mode, you can use that. In this mode, the multimeter will sound a tone whenever it detects a closed (unbroken) circuit.

Measurements you might need to take


You probably won't be called on to measure current. But you might need to measure voltage, resistance, or continuity.

You might need to check the output voltage of a power supply at various leads to verify that a component is getting the power it requires. You might also need to verify that appropriate wall voltage is available.

You will measure resistance most often when determining if a cable is whole or if a break exists. You might also need to determine if the appropriate size resistor is being used for an application.

Do it!

A-1: Measuring electrical values

 Make sure students follow proper electrical safety practices during this activity.

Provide students with batteries, power adapters, good and bad network cables, and so forth to measure.

Here's how	Here's why
1 Using a multimeter, determine the voltage being output by the various devices provided by your instructor	Your instructor will provide you with devices, such as batteries or power adapters, for which you can determine output voltages.
2 Determine the resistance of the various components provided by your instructor	Your instructor will provide you with cables and other components for you to measure.

Signal generation

Explanation

When testing audio/video equipment, you might want to create your own signal rather than relying on picking up cable or satellite delivered signals. Test signal generation equipment is available that will generate digital and analog signals. The test equipment enables you to set the parameters of the signal, so you are able to accurately test video levels.

Signal generators are also available that enable you to test audio signal levels. In addition, for wireless applications, since you can't "see" RF signals, a signal generator can create a sound (usually FM static) that indicates that the signal is present.

Cable testing devices

You can use a cable testing device, as shown in Exhibit 7-3, to test the physical cables and network functions. You can purchase cable testing devices for your particular LAN or purchase one that is compatible with multiple network types. For example, testing devices are available for 10 and 100 Base-T networks.

11



Exhibit 7-3: A cable testing device.



Examples of physical cable tests that your cable testing device might be able to perform include:

- Locating miswired cables
- Locating missing cables
- Locating cables that don't support your network type (for example, 100 Base-T)
- Testing hub connections
- Testing PC connections
- Testing installed cables
- Testing patch cables
- Locating and tracing inactive cables



Examples of network function tests that your cable testing device might be able to perform include:

- Verifying if PC is ON, if it appears as a PC and maximum speed
- Verifying if hub is ON, if it appears as a hub and maximum speed
- Verifying PC to hub speed and data transmission
- Verifying hub to hub data transmission
- Determining if straight thru or crossover patch cable is required
- Finding speed bottlenecks on LANs
- Monitoring LAN link between two devices

Do it!

A-2: Using cable testing equipment

Here's how	Here's why
1 Follow your instructor's directions to attach your cable tester to your computer's network cable	Your instructor will provide you with a basic cable tester. You will then test the section of cable between your PC and the hub.
2 Follow your instructor's directions to attach your cable tester to the network cable ending at the hub	
3 Follow your instructor's directions to test the section of cable and read the tester's display	
4 Follow your instructor's directions to remove the cable tester and reattach the cables	

Explain to students what problems their tester can find.

Troubleshooting

Explanation

Troubleshooting is the process of determining the cause, and ultimately the solution to a problem. By applying a logical, consistent method to the troubleshooting process, you make your job easier and shorten the time it takes to discover the root of a problem.



There are several popular models that you can follow when troubleshooting PC hardware problems:

- The CompTIA A+ troubleshooting model
- The CompTIA Network+ troubleshooting model
- The ASID troubleshooting model

All models incorporate basic troubleshooting theory. The stages of basic troubleshooting theory are included in the following table.



Stage	Description
Back up data	If there is the potential that the changes you plan to perform might make the data on the system inaccessible, back up data before making any changes.
Divide and analyze	Assess the problem systematically. If it is a large or wide-spread problem, divide the problem into smaller components to be analyzed individually.
Verify	Verify all aspects of the problem. Be sure not to overlook the obvious problems. Determine whether the problem is something simple. Remember never to make assumptions.
Research	Research ideas about possible solutions to the problem. Establish priorities for resolving the problem.
Document	Document your findings. This includes the actions you take and the outcomes of your actions, both for those solutions that worked and for those that did not work.

CompTIA's A+ troubleshooting model

The CompTIA A+ troubleshooting model has you complete steps to apply basic diagnostic procedures and troubleshooting techniques. CompTIA recommends completing the steps listed in the following table.



Step	Description
Identify	Identify the problem including questioning the user and identifying any changes the user has made to the computer.
Analyze	Analyze the problem including potential causes. You can then make an initial determination of whether it is a software and/or hardware related problem.
Test	Test components related to the problem. This includes inspecting them for obvious things such as connections and power being connected and turned on, hardware and/or software configurations, checking Device Manager for indications of conflicts or problems, and consulting vendor documentation for descriptions of status lights and other indicators.
Evaluate	Evaluate the results and take additional steps to correct the problem if necessary. Additional steps might include consulting with other professionals or the vendor, use of alternative resources, and reviewing the manuals.
Document	Document the activities you took in correcting the problem as well as the outcomes of the actions you took.

CompTIA's Network+ troubleshooting model

CompTIA recommends a troubleshooting model for network technicians. You can follow this process for computer repair as well. It consists of the eight stages in the following table.



Stage	Description
Identify the exact issue	Use open-ended questions to query the customer to determine the precise nature of the problem.
Re-create the problem	Have the customer repeat the action or demonstrate the problem. Alternatively, you can follow the steps to re-create the problem.
Isolate the cause	Eliminate factors that are obviously not part of the problem. Then, starting with the most likely cause of the problem, begin to identify the cause.
Formulate a correction	Determine one or more solutions to the cause that you've identified.
Implement the correction	Implement the correction. If this doesn't solve the customer's problem, undo any changes you made. Then, working with the next most likely cause, formulate a correction and implement it.
Test the solution	Make sure that your solution actually fixed the problem. Verify that the user agrees that you have fixed his or her problem and that the solution has not caused other problems.
Document the problem and solution	Create a detailed record of the problem and eventual solution. You will be able to use this documentation in future troubleshooting situations.
Provide feedback	Using your assessment of the customer's interest and technical understanding, describe to them the exact cause and solution to the problem.

Tell students that they may need to repeat stages 4–6 until they discover and fix the true cause of the problem.

The ASID troubleshooting model



The ASID troubleshooting model offers a four-stage process that you can apply to many types of problems. Its stages are:

- 1 **Acquire** — Acquire information about the problem.
- 2 **Simplify** — Remove any non-critical components.
- 3 **Implement** — Identify and implement potential solutions one at a time.
- 4 **Document** — Document the problem and its resolution.

In the Acquire stage, you collect information about the problem. During this stage, you:

- Elicit symptoms of the problem from the user.
- Have the user repeat the activity that caused the problem to reproduce the error for you; document the exact steps that caused the problem.
- Identify any recent changes to the system and its configuration.
- Document any error codes that are reported by the system.

In the Simplify stage, you remove any non-critical components, such as unnecessary peripherals, shut down unnecessary running programs, disconnect from the Internet or network, and so on. If the problem goes away, its cause lies with one of the components you removed. If not, then you have simplified the system, which will make troubleshooting easier.

In the Implement stage, you identify and implement potential solutions one at a time. Check available reference materials for potential solutions. Available resources might include:

- User/installation manuals and product documentation
- Internet/Web resources, such as manufacturers' Web sites and users' forums
- Training materials

Make sure to document any changes you make on the system. If a particular change doesn't fix the problem, undo your change and try another solution.

The Document stage occurs throughout the other stages and finishes after you have a resolution to the problem. During the previous stages, you documented the error symptoms, the components you removed from the computer, and the solutions you tried and whether they were successful. At the end of this process, you must fully document the resolution for later reference. It's just as important to record any significant or obvious solutions that turned out not to be the cause of this problem so that you can avoid dead ends in the future.

Documentation

Documentation is the key to the success of any troubleshooting model you choose to follow. Such documentation takes two forms: that which is provided by others and that which you create.

You will find product manuals, manufacturer Web sites, and technology-related knowledge bases to be invaluable sources of information when troubleshooting problems. You should consult these references early in the troubleshooting process to determine if you're dealing with a known problem with a previously published solution.

Problems that you must solve will often be specific to your customer's combination of hardware and software, as well as to how they use their systems. Your notes will be the best reference for future problems because they will apply specifically to your customer's environment.

You must consider the following factors when determining the best documentation solution for your needs.

Item	Description
Paper or software	You must determine which is best for your needs, a paper-based or software-based record of problems and solutions. Paper logs are well suited for one or two-person troubleshooting teams. You will probably need to turn to software solutions for larger or distributed troubleshooting teams. If you use a software-based system, you must consider how to maintain the information and make it available during a computer outage or after a disaster.
Organization scheme	How you organize your log information will determine how you can find the data later. If you're using software, it will determine which scheme or schemes you must use. If you're using paper, you could organize your notes by hardware component, by software application, by problem symptom, by user or department, by location, or other scheme.
Level of detail	Only you and your troubleshooting team can determine how much information to record. If you do not record enough detail about the problem and its solution, the documentation will be useless for solving future similar problems.

Referring to prior documentation

It is helpful to know if the system has had problems before and what the solution then was. Most troubleshooting methods include a step to document both the problem and the solution. An organized record of this information will help speed the troubleshooting process and help to provide faster resolution in the future when the same or a similar problem occurs.

Web site support

When you are troubleshooting a hardware or device problem, one of the first places most people turn is to the Web site for the product. They often have a page that covers frequently asked questions (FAQs), a knowledge base of known issues and the fixes for those issues, help and support which might be simply the documentation for the product or more robust support information.

The Microsoft Knowledge Base

When you're having a problem with software or hardware on a computer running a Microsoft operating system, an excellent troubleshooting reference is the Microsoft Knowledge Base. This Web site contains problem and solution references for Windows 2000 Professional, Windows XP Professional, Windows XP Home Edition, Windows XP Media Center, and many other Microsoft applications. Sometimes, it provides a hyperlink to an FTP site where you can download patches and new releases. The Knowledge Base explains many Microsoft error messages. You can enter the specific message in the Search box and retrieve a description of the error's cause and a solution for resolving the problem.

To access the Microsoft Knowledge Base:

- 1 Using Internet Explorer or another Web browser, go to support.microsoft.com.
- 2 Click Search the Knowledge Base.
- 3 Type a keyword or words for the search, and click Go.
- 4 To find more results, click the Back button in your Web browser, and select a larger number of articles in the Results Limit list.
- 5 Click Go.
- 6 Click an article to read it.

You can print articles or save them to your hard disk for later reference.

Communicating with technical support

If you can not figure out the solution to the problem using your troubleshooting skills, the documentation, records of past problems or the support documents from the company's Web sites, you might need to contact the company's technical support personnel.

They will often go over the same ground that you already covered in your own troubleshooting attempts, but in order for them to make sure that no possible solution is left untried they usually start from the beginning and walk you through all of the possible solutions from the simplest explanation and going up through progressively more complex possible solutions.



There are often multiple tiers of support personnel at the company.

- The first line of support personnel usually works from past problems and known issues databases.
- The next level of support has somewhat more technical documentation to work from and usually more experience with the software or hardware being supported.
- A third tier of support personnel are called in when neither of the first two tiers can figure out the solution. They often try to replicate the problem and work either with you on the phone, or contact you later when they have had time to work on the problem.

Demarcation and responsibilities of associated trades and utilities

The demarcation of your equipment versus the service provider is usually clearly visible. Any boxes they rent to you are considered theirs. This typically includes items such as cable modems, satellite receivers, and digital phone modems. The cables, including phone, cable TV, and electric utility all are serviced to the point where they enter your house and are the responsibility of the service provider. Once the cable, wiring and so forth are in your home it is your responsibility to protect it using proper surge and wiring protection to keep it in working order.

Do it!

A-3: Troubleshooting problems**Questions and answers**

- 1 Which troubleshooting model is best and which is worst? Why?

None is inherently better or worse, though one may be more applicable to a particular circumstance.

- 2 Hector reports that his computer doesn't work. Using either CompTIA model, describe the first step you would take to fix his problem.

First, you should identify the exact problem through a series of open-ended questions. For example, "What isn't working?" or "Can you describe the problem to me?"

- 3 Isabelle calls you to say that her A/V system is not broadcasting to the bedroom. Following the ASID method, what would your first steps be?

After acquiring exact information, such as the applications being used and any error codes, you should simplify her system. Disconnect any devices that are not being actively used and see if the problem remains.

- 4 What documentation should you record once you've found the solution to Hector's and Isabelle's problems?

Answers will vary, but should include:

- *The error symptoms*
- *The components you removed from the computer*
- *The solutions you tried and whether they were successful*
- *A fully documented resolution for later reference*
- *Any significant or obvious solutions that turned out not to be the cause of this problem so that you can avoid dead ends in the future*

- 5 A user calls the Help desk because her lights are turning on whenever her wireless doorbell rings. What should you do first in the ASID troubleshooting method?

Acquire. Begin to collect information about the problem from the user.

Topic B: Troubleshooting wireless systems

This topic covers the following CEA-CompTIA DHTI+ exam objective.

#	Objective
6.1	Identify and apply the fundamentals of troubleshooting and diagnostics. <ul style="list-style-type: none"> Troubleshoot common wireless interference issues

Troubleshoot common wireless interference issues

Explanation



For wireless connections, you need to determine the name of the network to which you're trying to connect. The View Available Wireless Networks option from the adapter's context-sensitive menu lists all of the networks that the adapter can detect. If you try to connect to the network and are denied access, you need to determine whether it requires specific security configurations, such as WEP or WPA. The administrator supporting the wireless access point or wireless router can give you the information you need or let you know if you aren't authorized to access that wireless network.

Some notebook computers have a switch to turn off the power to the wireless network adapter. This is so you don't consume extra power when you're using battery power and not connected to a wireless network. Be sure to turn this back on when you do want to connect to a WLAN.

If you've determined that the network is accessible and that you've configured your security settings as appropriate to that WLAN, then you should check whether your wireless adapter antenna is up and pointing towards the signal. On Windows XP computers, you can check the strength of the wireless signal by placing your mouse over the wireless connection icon in the system tray. A pop-up displays a summary of your wireless connection. If you click on the icon, it opens the Wireless Connection Properties box, as shown in Exhibit 7-4, which will also give you the summary information for your connection. If the signal is non-existent or weak, try moving closer to the WAP or router if possible. Some cards don't have an external antenna.

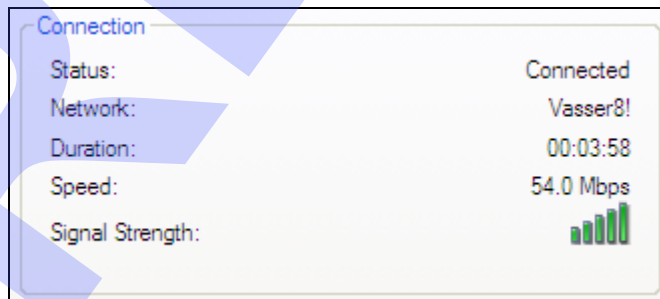


Exhibit 7-4: Wireless connection summary information

On laptops, these functions are often on a chip on the motherboard. If this has been damaged, you can get the same functionality by installing a PC card or mini-PCI card – whichever is appropriate to your laptop.

On desktop systems, wireless access is either through a PCI card installed in the system or via an external USB device. If you determine that one of these devices has failed, replace it with another working component.

Do it!

B-1: Troubleshooting wireless interference problems

Questions and answers

- 1 What is the first thing you should check if your wireless network is not working

Determine if you are connected and if so, the signal strength.

- 2 List some of the sources of interference for wireless networks.

Other radio signal sources such as cell phones, radio transmitters, pagers, electric grids, large motors, and other devices

- 3 What are some of the other devices with which a wireless network might interfere?

Pacemakers, aircraft control systems, and other sensitive electronic equipment

Other wireless connections

Wireless access using radio signals, infrared transmission, or beamed signals are all possible connection types in a home technology integration system. It is easy to install, so it is often used for connections in both computer networks and security systems. However, it is often subject to interference from other radio signal sources such as cell phones, radio transmitters, pagers, electric grids, large motors, and other devices. Wireless networks may themselves interfere with some devices such as pacemakers, aircraft control systems, and other sensitive electronic equipment.

One of the first things to check is that the device is receiving power. Put in fresh batteries in battery operated devices. Check that the outlets the transformers are connected to are receiving power. If they are connected to surge strips or UPSs, make sure the power is turned on.

If the device is configured using Unit and House codes or a channel selector, make sure they are set to the correct codes or channels. Failure to set the correct channel code will prevent proper operation. For example, an X10 system requires unique Unit codes for each device, but in order to communicate between devices, they all need to be set to the same House code. For A/V sharing devices, you usually need to select a channel on the receiver and set the TV to that same channel in order to receive the broadcast from the camera or remote TV.

If the devices causing interference cannot be removed from the area, you can try installing filters to eliminate or at least limit the interference. Some of the filters are low cost and easy to install; others require installation by a licensed electrician.

X10 data packets can be blocked by other carrier-current devices, including wireless intercoms. They can also be blocked by power-conditioning equipment such as power strips, computer power supplies, and other devices. An X10 device called a choke can overcome this problem, but finding where to place the choke can be difficult. Interference from an outside source is also a potential problem for X10 signals. An expensive signal block may be required to filter such outside signals. Signal block installation is also costly and must be done at the main service panel by a professional electrician. Finally, appliances in the home can generate interference or block X10 signals entirely. Such devices require noise filters to correct the problem.

Minimizing high-voltage interference

Explanation



High-voltage interference in a home LAN can originate from a number of sources and affect several parts of the network.

Outside interference can be caused by lightning and the atmospheric conditions that produce it. Wind can also generate static electricity, either by the friction of air moving over stationary objects or by the motion that wind pressure produces in everything from tree leaves and flags to tumbleweeds and windmill blades. Other sources of interference from outside the home include radio stations, citizens band, and police radios, and inside the home, sources include household appliances and fluorescent lights.



Inside interference is mainly produced by differences in electrical potential between different parts of the home or between objects in the home. These differences cause electric currents to flow for very short periods of time between some of the points with differing potential. The brief electrical flows tend to neutralize the potential between the different points, but the current flow often passes through wires, metal component parts, and other conductors that form part of the network structure. When this happens, the high voltage of the flow disrupts the low-voltage flow of data in the network, or may even entirely obliterate it for a time.

Interference can also be caused by operating pieces of electrical equipment that create electromagnetic fields around themselves. Imperfectly wired electrical connections can produce tiny current arcs. These arcs result in interference being generated around the circuit.

Finally, almost any movement of an object through the air or while in contact with another object can generate a static electric charge on the object which when discharged produces interference. This can mean anything from feet walking on a nylon carpet (and discharging with a painful spark when the walker touches a metal object) to clothes tumbling in the drum of an automatic dryer.

Static electric discharge, correctly termed *electrostatic discharge (ESD)*, occurs whenever the static charge on two objects is dissimilar. If the two objects touch, electricity from the one with the higher voltage charge flows to the one with a lower voltage charge until the two charges are equalized. Static discharges can attain very high voltages. If you touch a metal object and feel an electric discharge, the static charge (voltage difference between you and the object) was 3,000 volts or more. If you saw a spark when the discharge occurred, the voltage difference was at least 8,000 volts.

Such voltage discharges can produce high levels of interference and also damage or destroy low-voltage electrical circuits and parts that normally function in a voltage range of five volts or less. Even a mild static discharge can wipe out a data packet running in a low-voltage wire, or completely fry a milivolt-rated capacitor or other electronic part.

Static charges can also be produced by high-voltage devices. All cathode ray tubes (computer monitors, television screens) contain high-voltage electron beams and create static on the face of their screen and also on surrounding objects. Laser printers, copiers, and power supplies in computers and many types of electronic equipment all produce static charges as part of their normal functions. These static charges can remain for long periods on the equipment even after power to it is shut off. The charge can also transfer to other objects or people, creating interference as it does so and forming a new voltage difference on the object or person that can then create more interference when it discharges again.

Finally, fluorescent lights produce interference through a phenomenon called electromagnetic induction (EMI). The high-voltage transformer, called a ballast, in a fluorescent light causes an electromagnetic field to be generated around the transformer by the current passing through it. This field is what causes a fluorescent light to glow. It induces a current to flow through the fluorescent tube, causing the phosphorus inside the tube to emit light. The electromagnetic field can also induce a similar current in other nearby objects, including network cables and electronic equipment. This is why network cables (and other low-voltage wiring) must never pass close to fluorescent lights or other high-voltage devices. Induction currents in the network wiring can destroy data and can damage equipment if the discharge reaches it.

How much the interference generated in and around a home affects a home LAN depends on climatic conditions in the area (dry, windy conditions produce more static electricity and hence more interference), its location (proximity to radio stations, power lines, industrial plants), and how well the home is constructed to deal with the causes of interference. Most interference can't be prevented, but it can be minimized and its danger to the functioning of the home LAN almost entirely eliminated by careful wiring, good grounding, and perhaps a few filters.

The first defense against interference is to create as little of it as possible. Clean, securely connected wires and adequate separation of low-voltage lines from high-voltage equipment and circuits reduce interference. So does good maintenance of electrical equipment. Devices with electrically connected moving parts such as motors, relays, switches, solenoids, and sensors all produce interference if their parts are worn or dirty. Keeping all the home's electrical systems, not just the network-connected devices, in top working order minimizes the interference that must be dealt with after the fact.

The next step to zero interference is to ground everything electrical. Again, this applies to all the electrical devices in the home, not just those connected to the network. It may even apply to a few non-electrical objects, if you suspect that static charges are being generated on their surfaces. A carefully installed ground wire won't harm any object and may reduce interference on the network by eliminating a source that can't easily be filtered because it is not part of a circuit.

Floor surfaces, furniture, and glass don't ground well, but they all take a static charge quite readily. If these surfaces are near network wiring or devices, they can bleed interference into the network. Antistatic sprays, grounding mats, and removal, where possible, are all methods of eliminating this type of interference. You must determine on a case-by-case basis whether it is easier to eliminate a source of interference or filter it out after it is created.

For the interference that remains in a home after as many sources as possible have been removed, two other defenses remain: shielding and filtering.

Shielding

Shielding applies primarily to the network's cables and is actually a refined form of grounding. The data-carrying wires in a shielded cable are surrounded for the full length of the cable by a webbing of metal wires. Interference entering the cable through its insulation is intercepted by the Web of shielding wires and grounded before it can reach the data-carrying wires in the cable. If shielded cable is used in the network, it is important that the connectors are all properly attached so that the shielding is grounded and can discharge any electrical interference it intercepts. If the shielding isn't grounded, it can accumulate an electrical charge and eventually discharge part of it into the data line.

Twisted-pair cable also helps eliminate electromagnetic interference induced in the cable by proximity to AC power lines or equipment. This isn't as big a problem for most home LANs as it is in commercial networks, but wherever network wiring comes near AC wires or devices, shielded twisted-pair (STP) cable is a must.

Filtering

Filters are electronic devices designed to permit the normal function of a device, but block or suppress any other signal coming from it. Filters can be placed on either the source of interference (the preferable location, if it can be found) or on the recipient of the interference. The latter is the usual practice because the sources of interference are often impossible to locate.

AC power-line filters are often built into high-quality surge and spike suppressors. They allow the AC current powering a device to pass, but block any other frequency of signal. They are designed to be placed on equipment that might produce power-line interference or network devices that may be the recipient of the interference. One multiple outlet filter/suppressor can protect up to half a dozen devices for a reasonable cost.

Radio frequency interference (RFI) generally originates outside the home, and enters the LAN through a telephone or cable modem. An RFI and electrical noise filter placed on the incoming connection cable in front of the modem (so the incoming signal passes through the filter before reaching the modem) can eliminate this type of interference. These filters cost around \$100 but can greatly speed up a modem connection with serious interference by eliminating the need to resend many data packets corrupted by interference. The filter can also reduce lost connections to the ISP caused by interference.

An interference filter can also be wired into the network itself. These filters (which also often function as surge and spike suppressors) operate by eliminating high voltage from the network lines. Since network data is transmitted at plus or minus 5 volts, the filter simply suppresses any voltage significantly above that level and thereby eliminates interference. The key to good suppression is speed, and a quality network filter should act within a couple of picoseconds in order to block interference effectively. Network filters cost about \$50.

Do it!

B-2: Finding sources of static electricity and interference

Questions and answers

Use the following scenario to answer the questions below. You will try to figure out if any equipment is producing interference.

You have installed a wireless automation and security system for a client, and it works well, except that there seems to be a lot of interference that occasionally prevents some modules from performing properly. You think it is caused by something electric operating at intervals and producing the interference.

- 1 Take an FM radio outside and with the volume turned up high, tune the dial to the quietest location where no station is operating.
- 2 With the radio tuned to this location, walk into the building and hold the radio very close to each piece of operating electrical equipment.
- 3 Determine if you hear static on the radio when it is near equipment.
- 4 What would the static indicate?

You are hearing RFI produced by the equipment.

- 5 How could you silence the static producers and stop the network interference?

Install a power-line filter, often included in surge and spike suppressors. You can also place RFI filters on incoming connections through cable or telephone modems.

Topic C: Troubleshooting integrated subsystems

This topic covers the following CEA-CompTIA DHTI+ exam objectives.

#	Objective
6.1	<p>Identify and apply the fundamentals of troubleshooting and diagnostics.</p> <ul style="list-style-type: none"> • Use of testing equipment <ul style="list-style-type: none"> • Telephone butt set • Toner
6.2	<p>Given a scenario, demonstrate how to apply troubleshooting skills to integrated subsystems.</p> <ul style="list-style-type: none"> • Networking • Audio/video • Telephony • Security • Home control

Network troubleshooting

Explanation



A hardware support technician usually isn't responsible for network troubleshooting. However, you may be called in to help determine if the workstation or the network is the location of a problem.

Identifying the scope of the problem

When trouble calls start to come in from multiple people about not being able to connect to a network location, you can be pretty sure that the problem is with the network and not with the workstation, provided that the users were able to connect previously. If only a small group of users is affected, and if they're located in the same general area, you can usually trace such a problem to the hub to which they're all connected or to a cable leading to the hub. If the problem is with an individual user, then chances are you're the one to resolve the problem, because it's something within the workstation or the cable leading from the hub to the workstation.

Knowing the scope of the problem (whether it affects all users, some users, or individual users) you have some idea of where to start in troubleshooting a connectivity problem. For example, if the user can connect to the Internet but can't access e-mail, then the problem lies towards the application. On the other hand, if the user can't connect to any resources on the network, then you should look at the connection protocol configuration and the physical (or wireless) connection medium. Also, if you know that several users are having the same problem, then it's unlikely that the NIC configuration is incorrect or that the NIC is bad.

Observing status indicator lights

Most networking devices have status indicator lights that you can observe to see if the device is working. Typically the lights are green if the device is sending or receiving data properly.

NIC indicator lights

Many NICs have indicator lights that flash when data is being sent or received. Some have another light to indicate that there's a working connection to the network. If these lights aren't illuminating, you should check the configuration of the card to see if that's the problem. You can do so through Device Manager. The network card should display in Device Manager without any error or warning icons. In Exhibit 7-5, the LAN network card is reported as functioning, but the wireless adapter is reported as disabled.

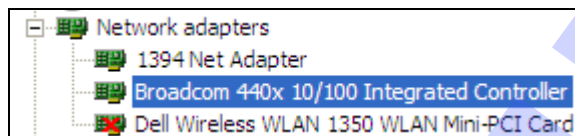


Exhibit 7-5: Device Manager displaying the status of NICs

The General tab of the NIC card's Properties sheet will also display the device's status. It should display "This device is working properly." as shown in Exhibit 7-6.

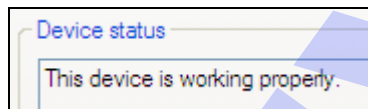


Exhibit 7-6: NIC card's Device status

Networking device indicator lights

If the port on the hub isn't receiving data, its indicator light isn't lighted. If all of the other ports on the hub are working, try swapping out the cable. You can also try connecting the cable to another port. This helps you determine if the problem is with the cable or with the port.

Checking TCP/IP communication

The ping command is useful in determining whether the user can access any other network devices or Internet locations. If the ping command fails, you should check the configuration of the IP address and verify that it's correct for your network. Next, check that the NIC is working properly. Then, check the network cable from the computer to the hub. Exhibit 7-7 shows an example of using the ping command.

```

C:\WINDOWS\system32\cmd.exe

C:\>ping course.com

Pinging course.com [198.80.146.30] with 32 bytes of data:
Reply from 198.80.146.30: bytes=32 time=96ms TTL=109
Reply from 198.80.146.30: bytes=32 time=94ms TTL=109
Reply from 198.80.146.30: bytes=32 time=87ms TTL=109
Reply from 198.80.146.30: bytes=32 time=87ms TTL=109

Ping statistics for 198.80.146.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 87ms, Maximum = 96ms, Average = 91ms

C:\>_

```

Exhibit 7-7: Results of the ping command.

If your computer network contains coax segments, a break anywhere in the cable results in users being unable to reach network resources. Remember, coax needs to be able to reach the terminated end of the segment, and any break in the cable prevents that from happening. Special cable testing equipment is used by network technicians to locate a problem cable in this type of network.

The `tracert` command is another useful networking command when it comes to troubleshooting. At the command prompt, enter `tracert destination_address`, where the `destination_address` is either the server name or IP address you're testing. You can determine how far the communication gets before the data can go no further. If the data gets onto the network and through the router, you can tell that the problem is beyond the local connection between the hub and the workstation. In such a case, call in the network support technician to locate where on the network the problem is occurring. Exhibit 7-8 shows an example of using `tracert`.

```

C:\WINDOWS\system32\cmd.exe

C:\>tracert course.com

Tracing route to course.com [198.80.146.30]
over a maximum of 30 hops:
  0  22 ms  1 ms  1 ms  192.168.2.1
  1  9 ms  8 ms  7 ms  10.108.80.1
  2  7 ms  6 ms  8 ms  24.93.3.109
  3  10 ms  9 ms  9 ms  srp7-0.rochnymth-rtr04.nyroc.rr.com [24.93.3.118]
  4  9 ms  15 ms  17 ms  srp3-0.rochnymth-rtr02.nyroc.rr.com [24.93.3.178]
  5  19 ms  18 ms  16 ms  son0-0-3.albnywav-rtr03.nyroc.rr.com [24.92.224.178]
  6  27 ms  19 ms  17 ms  pop1-alb-P2-0.atdn.net [66.185.133.233]
  7  19 ms  19 ms  19 ms  bb1-alb-P0-0.atdn.net [66.185.148.96]
  8  23 ms  22 ms  23 ms  bb2-nye-P3-0.atdn.net [66.185.152.71]
  9  26 ms  20 ms  21 ms  pop1-nye-P1-0.atdn.net [66.185.151.51]
 10  21 ms  21 ms  21 ms  0.so-2-2-0.BR1.NYC4.ALTER.NET [204.255.169.41]
 11  21 ms  21 ms  30 ms  0.so-6-0-0.XL2.NYC4.ALTER.NET [152.63.21.82]
 12  58 ms  58 ms  58 ms  0.so-6-2-0.CL2.CMH2.ALTER.NET [152.63.68.193]
 13  58 ms  57 ms  58 ms  188.ATM7-0.GW2.CMH2.ALTER.NET [152.63.66.149]
 14  63 ms  63 ms  63 ms  65.206.182.82
 15  74 ms  *  83 ms  nsu143055.thomsonlearning.com [198.80.143.55]
 16  65 ms  63 ms  63 ms  www.mycourse.com [198.80.146.30]

Trace complete.

C:\>

```

Exhibit 7-8: Using `tracert` to investigate the path to a destination



Remote connection problems

If you're using a dialup, DSL, or cable connection, problems can occur anywhere from the ISP, down the communication line to your building, down into the line within the building to the modem or transceiver, to the connection from the modem or transceiver to your computer, to the modem or NIC in your computer and its configuration. That connection contains a lot of areas you need to check to locate the source of the problem.

If you are using dialup, you can check the phone line by connecting a phone and seeing if you can get a dial tone. If you're using cable lines that also bring in cable television signals, see if the TV is receiving signals. Check the indicator lights on the transceiver or modem to see if any signals are being sent or received.

If it's determined that the modem or transceiver is working properly, you can try swapping out the cables connecting them to the service and to the computer.

Using a surge protector UPS that includes connections for telephone and cable lines can help prevent damage to the devices and computers using those lines. This device can help prevent damaging a transceiver, a modem, or a NIC in the path of a surge.

Do it!

C-1: Troubleshooting network subsystems

Questions and answers

- 1 How would you determine if the workstation can successfully connect to support.microsoft.com?

Using a Web browser you would determine if you could access the Web site. Next, you may also use the ping command to access the Web site.

- 2 What command would you use to determine how far the data packets can reach?

Use the tracert command to do this.

- 3 What are some things to try if your cable connection isn't working to connect to the Internet?

If the cable also supplies your TV signals, see if you can tune in channels on the TV. Check the indicator lights on the cable modem. Try swapping out cables connecting the cable line to the cable modem and/or from the cable modem to the computer's NIC.

A/V system maintenance*Explanation*

Video and audio systems are combinations of electronic and mechanical components and as such are subject to the same wear and environmental problems that afflict other similar devices. Because video and audio systems must continually operate at peak performance levels in order to produce quality output, even small maintenance problems can cause a serious degradation in their output. Electronic systems are adversely affected by three main factors: heat, water, and electric power variations. Mechanical systems are also adversely affected by these three and a fourth: dirt.

- Video and audio systems produce heat which needs to be dissipated or it will build up in components until they burn out. Many components contain heat sinks to help prevent heat build-up, and most systems provide for cooling with ventilating fans that carry heat away from the components. These work well if not obstructed by placement of the system in an enclosure where air circulation is restricted. Components should not be stacked on top of one another or enclosed so that the cooling fans in components can't circulate air freely. Likewise, components shouldn't be placed where they are subject to additional heat from outside sources such as heating fixtures, fireplaces, and space heaters. Keep the system in as cool an environment as possible and its own cooling components will maintain a good working temperature inside.
- Water problems for video and audio systems usually occur in the form of condensation of moisture from the air on internal components. This usually happens when the system is turned off and warm parts cool down, picking up condensate from the air as they do so. If the system is again turned on before the condensed moisture has had time to evaporate, short circuits or other damage to electronic parts can result. The key to avoiding condensation in a system is the same as for avoiding heat buildup: keep good air circulation within the components. The less heat buildup there is in the system, the less danger of condensation when it cools down. Likewise, the more air circulating in the system, the less chance there is for moisture to accumulate. This is another reason to keep systems out of areas or enclosures where slow-moving, moisture-laden air can create condensation.
- Power fluctuations are the surest way to damage a video or audio system, just as they can damage computer systems. High-quality, fast-acting surge suppressors are a must for video and audio systems. Voltage drops should also be avoided. This may mean connecting the system on an independent circuit and making sure that the home's power load requirement doesn't periodically pull down the voltage as equipment starts up.
- Finally, dirt, usually in the form of dust particles, is to be avoided in all mechanical systems. It increases wear on moving parts and can sometimes bring them to a halt. Video recorder/player heads rotate at over 1,000 rpm. So do CD players, DVD players, and hard drives. All of these are motor driven and rotate on shafts set in precision bearings. Even small quantities of dust can shorten the life of these parts. A component's internal parts can't be cleaned of dirt. The most that can be done is to keep dirt away from the equipment and out of the air that circulates through it. The more dust free the interior of the home can be kept, the longer its electronic systems will last.

A couple of case studies

Let's look at an example of how to troubleshoot some typical audio/video system problems.

A client for whom you've recently installed a video system complains that the television set in his daughter's bedroom has serious audio problems. This is an analog set that's connected to the satellite digital decoder/converter, but it displays its picture and sound only in analog format. The client has added a DVD player to this television station, connecting it to the television's input jacks with RCA cables. The problem is that the audio volume for satellite reception is normal, but sound from the DVD player varies tremendously at a single setting. Sometimes it's normal, sometimes too loud, and sometimes so low that it can't be heard.

You check the wiring setup and confirm that the television has only monaural sound capability. It's connected to the decoder via a single coaxial cable input. The DVD player's left side audio output is wired via an RCA cable to the monaural audio input jack on the television. A second RCA cable connects the composite video from the DVD player to the input jack on the television.

Your job as the support technician in this scenario is to determine why the DVD sound is varying so much. You also need to determine the solution that can correct the problem.

A likely solution to this problem is that the variation in sound output from the DVD player is caused by the fact that only half of its audio output is being received by the television. DVD players all have stereo sound output. Connecting only the left side of the output to the television means that all of the right side sound is lost. This results in large volume variations that depend on the side of the stereo system from which sound output is coming. The solution is a simple RCA combination plug that has two input jacks on one end and that combines both inputs into a single plug on the other end. This plug allows both audio outputs to be combined in the television's monaural input and eliminates the sound variations caused by the missing audio output.

Let's examine another example.

A client with a satellite digital television receiver wants to add a second receiver to his system. Rather than purchase or lease a second decoder from the satellite company, he suggests installing a splitter on the existing decoder's output line and simply running its signal to both television sets. This saves him the installation cost and continuing fees for additional satellite service. He wants to know if this idea will work and what potential problems there might be.

Your answer might be that splitting the signal coming out of the decoder is possible, although doing it weakens the signal on both legs of the splitter and may require a signal booster if the cable connection to either television set is long. More importantly, splitting the signal after it passes through the decoder doesn't really provide another reception channel. The second television set connected to the decoder can only show the same channel that's playing on the first set. The channel can be changed only at the decoder, and both television sets will always display the same channel. If one set is located in a different room from the decoder, a viewer will have to go to the decoder room to change channels, because the controller for the decoder is a line-of-sight IR device that won't work from another room.

Even though this setup is possible, the customer won't be satisfied with it. A second satellite decoder should be installed for the second television set. It will be worth the cost.

Do it!

C-2: Troubleshooting audio/video subsystems

Questions and answers

- 1 List the three main factors that can adversely affect electronic systems.

Heat, water, and electric power variations

- 2 What is a fourth factor that affects mechanical systems?

Dirt

- 3 How are A/V systems cooled?

Heat sinks, ventilating fans, not stacking them, not placing them in enclosures where air circulation is restricted, away from external sources of heat

- 4 What sort of water damage is most often found on internal electrical components? Where does it come from?

Condensation. It occurs when the system is turned off and warm parts cool down, picking up condensate from the air as they do so.

- 5 What is the best way of protecting A/V systems from power fluctuations?

Using surge suppressors

- 6 How can you protect equipment from dirt?

Keep dust and dirt away from mechanical components such as video recorder/players, CD players, and DVD players.

- 7 After installing a new surveillance camera in a home, none of the existing TVs display the signal, even though you've programmed the modulator properly and checked all the connections. What is the problem? What other diagnostic procedures should be done? How can this be prevented?

Possible solution:

The first task is to hook up a monitor directly to the camera to verify that it's operating properly. Next, check for digital or high-speed services that are provided by the cable company. These can block other signals from modulators. The solution to the problem is to install a high-pass filter before the signal is distributed around the home or combined with the camera signal. The high-pass filter blocks the signals associated with digital or high-speed service, so the camera should be installed in a manner that it doesn't block those signals tracking to the areas that they need to be, for example, to the cable modem.

Troubleshooting telephony subsystems

Explanation

Phone technicians use network tone generators and butt sets to check the lines and extensions on the phone system. Using these tools, they can determine if the problem is at the phone, with the line or the jack, or at the main system.

Butt set

A *butt set* is a portable hand-held phone that has connectors that can be clipped to wiring blocks or plugged into the line jacks. In some cases, a butt set has simply a pair of alligator clips for making temporary connections, as shown in the following illustration. Many modern butt sets include an additional wire ending in an RJ-11 modular phone jack.



Exhibit 7-9: A butt set

A technician connects the butt set to a line, jack, or connector block and presses a button on the set to take the phone “off the hook.” He or she can then listen for dial tone, make a call, or even receive calls.

Toner and probe

To test the continuity of wires or trace out lines, technicians use a toner—also called a tone generator—and probe. A toner is a device that injects a high-pitched, often oscillating tone, onto a wire that can be received with the probe. The toner must be physically connected to the wires. However, the probe will emit the sound when it is brought near the appropriate wire.

When installed, wires are typically marked at both ends with identifying numbers or other labels. Sometimes those labels fall off or are never attached. A technician can find where a wire goes by attaching the toner to one end and then moving the probe around the various wires at the other end of the cable. When the tone is loudest, in most cases, he or she will have found the proper wire. Cross-connected wires or those that are shorted together will all transmit the signal, so further testing might be required to be sure the proper wire has been found and that it’s in usable condition.

A case study

Let's examine what you might encounter when troubleshooting telephony subsystems by looking at a case study.

The installer shows up for installation of telephone service, and the demarc hasn't been installed or the service isn't live. The result is the customer doesn't get a live phone service connection when he moves into the home. Customers usually view this as an urgent situation and call the installer.

Four parties are involved:

- The installer
- The service provider
- The service provider's installation crew
- The homeowner who has to instigate the service activation or switch

Note that the service provider won't touch the installer's wiring (the wires that go into the house). Even if the wiring is right in front of the service provider's installation crew, they won't connect it. Keeping this in mind, the installer has to watch out for the following scenarios:

Scenario 1: No demarc evident — The installer does his job wiring the home and must come back to connect the service. The installer leaves the wires coiled up in an opening that the contractor created for the demarc.

The installer has to come back from time to time to check for a demarc. If you're performing services on multiple houses in a development, visit the outside of the houses that you have installed and check for the demarc. It's just a few screws to open the box and connect the wires. However, this may not assure a working service if the homeowner hasn't activated it or if the service hasn't been switched on by the provider.

Scenario 2: Demarc is evident — The installer connects the wires at the demarc. The installer comes back after the homeowner has moved in and verifies that all systems are working. Sometimes, the homeowner forgets to transfer the service, so even if all the wires are there, the line may be dead.

Scenario 3: Homeowner moves in, but demarc isn't there! — Sometimes the demarc isn't installed even after the homeowner has moved in. In this case, the homeowner needs to contact the builder to get the demarc installed. After this installation, the integrator needs to return to connect the wiring to the demarc. Sometimes the service provider has activated the service, but the crew hasn't physically installed it.

Possible solution

To prevent these scenarios from occurring in your projects, be sure to have daily communication with the builder to be sure that the demarc is there. Establish a line of communication with someone at the service provider involved with scheduling the hookups.

Do it!

C-3: Troubleshooting telephony subsystems

Questions and answers

- 1 What are the two pieces of equipment needed to troubleshoot a wired telephone system?

A butt set; a toner and probe

- 2 Why might you use a toner and probe?

With a toner and probe, you can determine the continuity of a wire, trace its route and connections, and match the ends of an unlabeled wire.

- 3 What is a butt set and what is it used for?

A telephone handset that has connectors to fit line jacks and also clip to wire blocks. It is used to check line integrity.

- 4 What is a network tone generator and what is it used for?

An electronic device that sends proper voltage and dial tone into a phone systems wires so they may be checked for integrity

Explanation

Troubleshooting security systems

Security systems rarely break down. Their reliability is partly a function of good initial construction to meet the durability requirements of a quality system and partly due to the fact that their components have few moving parts and a very low level of activity. They simply observe and occasionally signal conditions around them. Security system components almost never wear out. Most service and maintenance for these systems center around their aging rather than mechanical or electronic breakdowns.

Security sensors are self-monitoring, sending a signal to the security panel periodically to confirm their functioning status. They also monitor their batteries and signal when power begins to drop off. Finally, if the condition that a sensor is monitoring changes, or something happens to the sensor to impede its monitoring of that condition, it signals an alarm. With this degree of self-monitoring, little external monitoring of sensors is ever needed. As long as their batteries are changed when signaled as low, sensors can function almost indefinitely without service.

Security panels also require little in the way of service or maintenance. They're generally AC-powered and have backup batteries that age over time. These should be changed every two to three years, even if never used. Like all electronic equipment, security panels can be damaged by power surges and spikes and should be protected by a surge suppressor on the AC circuit.

The response devices in a security system are the most vulnerable to maintenance problems and should be tested annually to see that they're still functioning well. Electronic speaker alarms rarely malfunction, but mechanical bells do and should be activated to confirm that they're working. The same is true of any mechanical response device that functions only if an alarm is signaled. Electric solenoids, motor-driven actuators, and especially valves, left unused for a year or more, can corrode and become frozen in their static position. They should all be activated periodically to be sure that they can activate when signaled to do so by the security panel.

As is the case with all electronic systems, the enemies of electronic security systems are heat, dirt, power spikes, and water. Wherever any of these can attack a part of the system, it should be protected as much as possible and regularly monitored for possible failure. Among the specific points in a security system that should be checked are:

- Wireless window detectors (for heat damage to the transmitters from sunlight coming through the glass)
- Outside motion sensors (for dirt or obstructions that may block all or part of their fields)
- Inside motion sensors (for dust and spider webs blocking their fields)
- Outside wireless sensors (for weather damage)
- Break switches on window and door sensors (to detect anything inserted in the switch to prevent its opening)
- Make switches on pressure pads or similar devices (to detect anything inserted in the switch to prevent its closing)
- Locks (to be sure they don't stick open)

A case study

Let's take a look at what might happen when you install and test a security system.

You're putting the finishing touches on a security system. During this process, you test each door and window to verify that it reads as open on the keypad when it's in the open position. Everything seems to be working except one window. When you open that window, the security keypad doesn't show it as open. You check the placement of the magnet and the sensor, and they appear to be correct. You test the wire for continuity, and it checks out.

You'll need to figure out the process needed to solve the problem as well as which tools you'll need to use. You'll also need to determine what other information would be important in solving this problem.

A possible solution to this problem is that more than likely caused by a nail or screw shorting out the wire somewhere behind the wall. The first thing to try is to disconnect the sensor and test the wire from that side. It should still show that it's shorted. A line tester can then be used to determine the distance from the end of the wire to the short. This is why it's important to have good documentation about how the wires are run in the home and the direction they take. Once the tester tells you the distance, then the wire can be traced and the short found. The drywall will have to be opened and the offending screw or nail removed.

System recovery

Explanation

If a security system signals a fire through one of its sensors, that sensor should always be replaced when the system is brought back into service after the fire. Fire and smoke sufficient to set off an alarm should always be assumed to be sufficient to damage the sensor so that it won't function as well in the future. These sensors aren't expensive, and the safe practice is to replace the possibly damaged sensor with a new one.

Fire damage to other parts of the security system, especially a wired one, should be carefully checked and, if necessary, repaired. Heavy smoke can damage some sensors even if fire doesn't reach them. Water damage is also a real possibility, particularly for wireless transmitters on sensors and the security panel.

Other sensors in a security system are rarely damaged by being activated. They can usually just be reset and used again. The possible exception is a water sensor, which may be affected if submerged for a long period of time. Again this isn't an expensive sensor, and to assure that it functions well, replacement may be the best policy.

If a security system is breached by an intruder, all of its sensors should be checked afterward to be certain that no attempt was made to evade or disable them. The fact that the system worked to signal an intrusion doesn't preclude the possibility that efforts were made to get around it in some other way.

False alarms can sometimes be very troublesome in security systems. Whenever they occur, they indicate the need for a service evaluation of the system. Eliminating the causes of false alarms makes the system more reliable and also makes the homeowner and emergency services more willing to rely on it.

False alarms can be partially prevented by careful wiring and installation so that signal failures don't occur as a result of poor connections. False alarms can also be generated from a number of innocent sources that are difficult to eliminate entirely. Outside motion sensors may be triggered by debris blowing in a high wind. Light beam sensors can be broken by a wandering cat or a sleepwalking child.

Window and door sensors can sometimes be tripped by strong winds flexing the door or window inward slightly, thus breaking the sensor switch.

There's no sure way to prevent false alarms entirely, but they can certainly be minimized by noting the conditions under which they occur and carefully trying to trace the cause. Adjusting or repositioning a sensor may be all that's needed to correct the problem. If not, changing to a different type of sensor may be an answer or simply eliminating one troublesome sensor and covering the area with other devices in different locations. If false alarms happen only at night or only with sensors that can't be easily observed by those inside the home, the possibility that someone is deliberately testing the security system's effectiveness shouldn't be dismissed. False alarms shouldn't be used as a reason to turn off a security system.

Do it!

C-4: Troubleshooting security and surveillance subsystems

Questions and answers

1 Why do security systems rarely break down?

They contain few moving parts and have a very low activity level.

2 How do security sensors monitor themselves?

By sending a signal to the security panel periodically to confirm their functionality. Battery-operated components signal when power drops off.

3 What maintenance should be performed on security panels?

Change batteries every two to three years.

4 Which components are most vulnerable to maintenance problems?

Response devices

5 How often should they be tested? Why?

At least annually. They can corrode and become frozen in their static position.

6 Why should a fire detection sensor be replaced after a fire?

Fire and smoke sufficient to set off an alarm is enough to damage the sensor.

7 What other sensors might need to be replaced after being activated?

Water sensors

8 List some causes of false alarms.

Answers might include:

- *Poor connections*
- *High winds blowing debris or causing door/window frames to flex, thus breaking the sensor connection*
- *People or animals wandering around during the night*

9 What are some things to try in preventing false alarms?

Answers might include:

- *Adjusting or repositioning sensors*
- *Changing to a different type of sensor*
- *Eliminating the offending sensor and covering the area with other devices in other locations*

10 If you get too many false alarms, you should just turn the security system off.
True or false?

False

Home control

Explanation



Problems with automated lighting systems X10, Zigbee, and Z-Wave, come mainly from interference or attenuated signals. For X10, the separation of the two legs of the home's electrical system can also be a problem.

AC electrical service to homes arrives as a 220-volt current that's divided into two legs of 110 volts each. One of these legs powers each of the home's 110-volt circuits and both power the 220-volt circuits to appliances such as the stove, clothes dryer, and other 220-volt devices. Both legs of the AC power work together in most homes, but they may not be actually joined in a manner that allows the higher-frequency X10 signals to travel easily on both legs. If the signals can't move freely on both legs, then they're likely not to reach some control modules on one leg or the other. This failure results in some control commands not being implemented.

The solution to this problem is an X10 bridge installed on the in-house side of the service line. This bridge connects the hot wires of both legs of the house AC current to one another. The bridge can be installed at the electric service box by an electrician. However, a new model is now available that can be installed by a homeowner or technician on any 220-volt outlet (such as for a stove or clothes dryer). The bridge, which is an X10 accessory available from several manufacturers, provides a path for X10 signals to reach control modules on both legs and should eliminate the problem of one leg transmitting no signals or the problem of signals too weak to be read by the control modules.

Weak X10 signals can also occur in a home with a large AC electrical system. The signals attenuate with distance and eventually become too weak to be read. A regenerator, placed in an outlet some distance from the command modules but close enough to read their signals clearly, can solve this problem. It reads all command signals on the AC wiring and regenerates them at full strength without any interference or noise they may have picked up in transit. In very large homes, two regenerators, placed some distance apart from one another, may be needed to keep signals strong throughout the house, but in most cases a single unit is enough.

Even with a bridge and a signal regenerator in place on the AC wiring, some X10 control modules may have trouble receiving commands from controllers. Among the causes of specific problems with individual control modules are the following:

- Reverse-wired outlets with the hot wire connected to the neutral side of the outlet and the neutral wire to the hot side. Correcting the wiring often solves the problem.
- Switched circuits in which the switch is on the neutral wire instead of on the hot wire. Again, correcting the wiring often solves the problem.
- AC suppresser or filter that blocks signals. Removing the blocking device is the only solution. Lighting circuits usually don't need suppressors or current filters, but if other equipment that does need one or both is on the same circuit, some rearrangement of connections may be necessary.
- Noise from other electrical equipment that interferes with the X10 signals. You can locate noise-producing electrical equipment using a radio tuned to a blank (no station) area of the broadcast band. A filter on the offending equipment often cures this problem, but if not, moving it to another circuit may be necessary.

- General noise that comes from an outside source that can't be eliminated. This type of interference is tough to combat. A filter on the incoming AC service line may help. Sometimes, an extra regenerator to keep the command signals well above the noise level works. If neither solution solves the problem, the only other option is to locate the source of the noise and somehow shield the home's wiring from it.

Wireless X10 systems can also be troubled by noise. RF frequency noise is difficult to filter out. Filtering each wireless receiver is simply too expensive and complex. The only workable answer is to find the source of the noise and filter that device.

Minor noise levels in wireless systems can usually be overcome by simply boosting the wireless signals so that they can be clearly read over the noise level. X10 signal regenerators are routinely used in large homes where signals attenuate, but these can also be used in smaller installations where their signal boost may be enough to overcome background noise.

A case study

Let's take a look at how a technician might deal with a lighting control subsystem problem.

You installed a power line carrier lighting control system in a new home. After your client moved in, he reports that the family room light goes on every night at 5 p.m., when it's programmed to go on at 6:30 p.m. After checking the programming, you verify that it states that the light should go on at 6:30 p.m. and off at 11 p.m. It's going off normally and no other lights are programmed to go on at 5 p.m.

You'll need to determine what the problem is. You will then need to solve the problem. In addition, you should figure out how to prevent the problem for occurring again after you have fixed it.

A possible solution is that there is interference from outside the house. Install a filter at the service panel of the home. This accomplishes two things. First, it stops unwanted signals from entering the home, and second, it stops signals from leaving the home and affecting the neighbors. By installing the filter, you'll solve most of the installation issues associated with power line carrier lighting control systems. If the problem persists, test the noisy items in the house. These include but are not limited to TVs, computers, stereo equipment, hair dryers, and any other devices that can create RF on the power line. However, in this scenario, it's unlikely that the interference is caused by those items since the problem occurs at precisely 5 p.m. every day.

Do it!

C-5: Troubleshooting automated lighting systems**Questions and answers**

- 1 Some lighting control commands aren't being carried out on your X10 lighting system. What solution could you implement to correct this problem?

Install an X10 bridge on the in-house side of the service line to connect the hot wires of both legs of the house AC current to one another

- 2 You've determined that the home has a large AC electrical system and that X10 signals are weak. What can you install to resolve the problem?

A regenerator placed in an outlet some distance from the command modules but close enough to read their signals clearly

- 3 RF frequency noise is easily filtered out. True or false?

False

- 4 How can you overcome minor noise levels in wireless systems

Boost the wireless signals with X10 signal regenerators.

- 5 In a home where you've installed an extensive X10-based automated lighting system, the client has added some X10-controlled shade openers and drapery pulls to the system. Everything works as programmed, except that, when one lamp module in the lighting system is commanded to turn on, one of the drapery pulls goes crazy. Sometimes it opens the drapes; sometimes it closes them, sometimes it moves them part way open or closed, and sometimes it appears to do nothing at all. If the lamp is turned off with another command, the movements of the drapery pull also stop. The drapery pull is normally activated with a handheld mini-controller, while the lighting system is controlled from a master controller in the family room. If the drapery pull is activated, the lamp also turns on and stays on, even when the drapes stop moving. What is wrong with the drapery pull? How can you fix the problem?

Possible solution:

Even though they're being activated by different controllers, both the lighting system and the drapery pulls use the same X10 signals. This problem is caused by having the drapery pull set to the same house and unit code as the lamp module in the lighting system. This causes both devices to activate on command from either controller. X10 drapery pulls respond only to On and Off commands. The seemingly erratic behavior of the drapery pull is actually just its normal operation. Any On command starts the pull moving to open or close the drapes, and it continues moving until it reaches the totally open or totally closed position, at which point its self-limiting switch stops it and reverses its direction. If an Off command is received, the pull stops in a partially opened or closed position. The next On command starts it moving again in the same direction it was going when turned off. The apparently random drape movements are really normal (but unintended) operation.

The problem can be corrected by changing the house or unit code on the drapery pull to one not used by the lighting system. This separates its operation from the lamp module.

Unit summary: Troubleshooting DHTI systems

- Topic A** In this topic, you learned to identify and apply the fundamentals of troubleshooting and diagnostics. You learned about the use of **multimeters** and **cable testers** in troubleshooting. Next, you learned about the importance of **prior documentation**. Finally, you examined **various troubleshooting models** and how to apply them.
- Topic B** In this topic, you learned how to troubleshoot common wireless interference issues. You examined how to **View Available Wireless Networks**. You also learned that on some notebook computers the **wireless adapters** can be switched off.
- Topic C** In this topic you learned how to apply troubleshooting skills to **integrated subsystems**. You examined how to troubleshoot a **network**, **audio/video sub systems**, **telephone subsystems**, **security systems**, and **home control systems**.

Review questions

- 1 What can you use a multimeter for?
You can use it to test continuity, voltage, and resistance.
- 2 What can you use a cable tester for?
To test the physical cables and network functions.
- 3 Why is prior documentation important?
It provides an organized record of this information that will help speed the troubleshooting process and help to provide faster resolution in the future when the same or a similar problem occurs.
- 4 What is the demarcation point for cables and wiring between the homeowner and service provider?
The cables, including phone, cable TV, and electric utility all are serviced to the point where they enter your house.
- 5 On Windows XP computers, how can you check the strength of the wireless signal?
By placing your mouse pointer over the wireless connection icon in the system tray.
- 6 You can check the phone line by connecting a phone and seeing if you get a _____.
dial tone
- 7 What does a green light mean on a NIC card?
The green light is a status light that means the network is connected and running.
- 8 What command is useful in determining whether the user can access any other network devices or Internet locations?
The ping command
- 9 Electronic systems are adversely affected by what three main factors?
Heat, water, and electric power variations

- 10 What is the most common problem that occurs with the three main types of home control systems?

Interference or attenuated signals

Independent practice activity

- 1 Your instructor will introduce one or more problems with the various classroom subsystems.
- 2 Identify the source of the problem.
- 3 Resolve the problem.
- 4 Verify that the subsystem is operating properly.
- 5 Document your work.

Appendix A

Certification exam objectives map

This appendix provides the following information:

- CEA-CompTIA DHTI+ examination objectives with references to corresponding coverage in this course manual.

Topic A: Comprehensive exam objectives

Explanation

This section lists all CEA-CompTIA DHTI+ exam objectives and indicates where each objective is covered in conceptual explanations, activities, or both.

1.0 Networking

Objective	Conceptual information	Supporting activities
1.1 — Identify basic networking protocols and their uses and know when/how to apply them.		
• DHCP	Unit 2, Topic A	A-6
• UDP	Unit 2, Topic A Unit 2, Topic D	
• DNS	Unit 2, Topic A Unit 2 Topic C	A-7
• TCP/IP	Unit 2, Topic A Unit 2 Topic C	A-6, A-7 C-1
• Subnet masks	Unit 2, Topic A	A-6
1.2 — Recognize and implement methods of network security.		
• Personal computer (PC) security	Unit 2, Topic A Unit 2, Topic B Unit 2 Topic C Unit 2, Topic D	B-2 D-3, D-4, D-5, D-6
• Antivirus	Unit 2, Topic D	D-2
• Home networking security	Unit 2, Topic B Unit 2, Topic D	B-2
• Firewall knowledge	Unit 2, Topic D	D-1
1.3 — Configure setup and maintain a residential LAN (Local Area Network).		
• Client configuration	Unit 2, Topic A Unit 2, Topic B	
– Resource sharing	Unit 2, Topic A Unit 2, Topic B	A-8 B-1 through B-5
– Peer-to-peer	Unit 2, Topic A	A-1
• Remote access setup	Unit 2, Topic C	
• Network device setup and integration		
– Broadband configuration	Unit 2, Topic C	C-1, C-2
– Routers	Unit 2, Topic A	
– Hubs	Unit 2, Topic A	
– Switches	Unit 2, Topic A	
– PoE (power over Ethernet)	Unit 2, Topic A	

Objective	Conceptual information	Supporting activities
1.4 — Configure setup and maintain a secure wireless network.		
<ul style="list-style-type: none"> Differentiate applications of hardwired vs. wireless networks 	Unit 2, Topic A Unit 2, Topic D	A-3
<ul style="list-style-type: none"> Assess networking security and encryption standards <ul style="list-style-type: none"> WEP WPA MAC filtering SSID WPA2 	Unit 2, Topic D Unit 2, Topic D Unit 2, Topic D Unit 2, Topic D Unit 2, Topic D	D-7 D-7, D-8 D-7, D-8 D-8 D-7, D-8
<ul style="list-style-type: none"> Wireless networking integration and troubleshooting <ul style="list-style-type: none"> Frequency management 	Unit 2, Topic D Unit 7, Topic B Unit 2, Topic D	D-8, D-9 B-1
<ul style="list-style-type: none"> Wireless protocol standards <ul style="list-style-type: none"> 802.11 a/b/g/n 	Unit 2, Topic D Unit 2, Topic D	D-7 D-7
1.5 — Identify and define networking cabling characteristics and performance.		
<ul style="list-style-type: none"> Cable types <ul style="list-style-type: none"> CAT5 CAT5e CAT6 Fiber Coaxial 	Unit 2, Topic A Unit 2, Topic C Unit 2, Topic C Unit 2, Topic C Unit 2, Topic C Unit 2, Topic C	A-4 C-3 C-3 C-3 C-3 C-3
<ul style="list-style-type: none"> Cable length limitations 	Unit 2, Topic C	C-3
<ul style="list-style-type: none"> Protocols <ul style="list-style-type: none"> 10BaseT 100BaseT 1000BaseT 	Unit 2, Topic C Unit 2, Topic C Unit 2, Topic C	C-3 C-3 C-3
<ul style="list-style-type: none"> Shielded (STP) vs. unshielded (UTP) 	Unit 2, Topic A Unit 2, Topic C	A-4 C-3
<ul style="list-style-type: none"> Plenum vs. non-plenum 	Unit 2, Topic C	
<ul style="list-style-type: none"> Importance of conductor colors 	Unit 2, Topic C	

2.0 Audio/video

Objective	Conceptual information	Supporting activities
2.1 — Implement, maintain, and troubleshoot multi-room audio systems. Identify common interference sources.		
• Control devices	Unit 3, Topic A	
– Keypads	Unit 3, Topic A	
– Rotary volume controls	Unit 3, Topic A	
– Sliders	Unit 3, Topic A	
– Push button controls	Unit 3, Topic A	
– Touch screen	Unit 3, Topic A	
– Wireless keypads	Unit 3, Topic A	
– Handheld devices	Unit 3, Topic A	
• Differentiate and define single source, multi-source, and local source	Unit 3, Topic A	
– Analog audio system	Unit 3, Topic A	
– Analog CAT5 audio system	Unit 3, Topic A	
– Digital CAT5 audio system	Unit 3, Topic A	
• Proper cable use	Unit 3, Topic A	
– Line level vs. speaker level	Unit 3, Topic A	
• Amplification	Unit 3, Topic A	
– Ohm’s law	Unit 3, Topic A	
– Watts vs. dB	Unit 3, Topic A	
– Local amplification	Unit 3, Topic A	
– Centralized amplification	Unit 3, Topic A	
• Speaker types	Unit 3, Topic A	
– In-wall	Unit 3, Topic A	
– Surface mounted	Unit 3, Topic A	
– Ceiling mounted	Unit 3, Topic A	
– Freestanding	Unit 3, Topic A	
– Fixed	Unit 3, Topic A	
– Animated	Unit 3, Topic A	
• Speaker specifications	Unit 3, Topic A	
– Frequency response	Unit 3, Topic A	
– Efficiency	Unit 3, Topic A	
– Power handling	Unit 3, Topic A	

Objective	Conceptual information	Supporting activities
2.2 — Install, configure, and maintain a residential home theater system.		
• Audio components	Unit 3, Topic A Unit 3, Topic C	C-1
– Define basics of acoustics	Unit 3, Topic A	A-1
– Audio/video components setup and integration	Unit 3, Topic A Unit 3, Topic C	C-1, C-3
– Multi-channel surround	Unit 3, Topic A	A-2
• Video components	Unit 3, Topic A	
– Display types	Unit 3, Topic A	A-3
– Hi definition resolution options	Unit 3, Topic A	A-4
– Tuner types	Unit 3, Topic A	A-4
– Video processing	Unit 3, Topic A	A-4
– Aspect ratios	Unit 3, Topic A	A-4
– Video setup	Unit 3, Topic C	C-3
– Digital video cable and connector types	Unit 3, Topic A	A-4
• MRAV (Multi-Room Audio Video) standards	Unit 3, Topic A	A-5
2.3 — Assess, install, and configure content management systems and describe their applications in a residential environment.		
• Describe typical applications and physical connection of sources	Unit 3, Topic B	B-1
– Media servers	Unit 3, Topic B	B-1
– Media PC	Unit 3, Topic B	B-1
– MP3 players	Unit 3, Topic B	B-1
– DVD players	Unit 3, Topic B	B-1
– Satellite	Unit 3, Topic B	B-1
– Cable	Unit 3, Topic B	B-1
– DVR	Unit 3, Topic B	B-1
– Gaming systems	Unit 3, Topic B	B-1
– Satellite radio	Unit 3, Topic B	B-1
– Legacy devices	Unit 3, Topic B	B-1
• Summarize types of media storage, methods to transfer, and backup data	Unit 3, Topic B	B-2
– Memory cards	Unit 3, Topic B	B-2
– NAS devices (Network Attached Devices)	Unit 3, Topic B	B-2
– Remote storage	Unit 3, Topic B	B-2
– Local storage	Unit 3, Topic B	B-2
– Frequency of backup	Unit 3, Topic B	B-2
• Other connection considerations	Unit 3, Topic B	B-3
– Digital Right Management	Unit 3, Topic B	B-3

3.0 Telephony/VoIP

Objective	Conceptual information	Supporting activities
3.1 — Differentiate and describe POTS vs. VoIP delivery. Identify and troubleshoot common issues.		
• VoIP	Unit 4, Topic B	B-1
– Compatibility issues	Unit 4, Topic B	
– Whole house distribution of VoIP	Unit 4, Topic B	B-2
– Performance and quality of VoIP	Unit 4, Topic B	B-3
• POTS	Unit 4, Topic A	A-1
– Cross talk	Unit 4, Topic A	A-3
– Radio interference	Unit 4, Topic A	A-3
– Dead ports	Unit 4, Topic A	A-3
– REN (Ringer Equivalence Number)	Unit 4, Topic A	A-3
3.2 — Describe and define fundamentals of telephone systems.		
• Multi-line	Unit 4, Topic C	C-1, C-2, C-3
• Paging	Unit 4, Topic C	C-3
• Intercom	Unit 4, Topic C	C-3
• Voice messaging/unified messaging	Unit 4, Topic C	C-3
• Door entry/gate entry	Unit 4, Topic C	
• PBX	Unit 4, Topic C	C-1
• Key systems	Unit 4, Topic C	C-2
• Telecommunication services	Unit 4, Topic C	C-3

4.0 Security and surveillance systems

Objective	Conceptual information	Supporting activities
4.1 — Install, maintain, configure, and troubleshoot basic security systems and applications.		
<ul style="list-style-type: none"> Define monitored and notification methods <ul style="list-style-type: none"> Phone line Cell phone Radio frequency IP based 	Unit 5, Topic B Unit 5, Topic B Unit 5, Topic B Unit 5, Topic B	B-1 B-1 B-1 B-1
4.2 — Describe basic security terminology and apply installation procedures and methodologies.		
<ul style="list-style-type: none"> Installation and configuration of security panel <ul style="list-style-type: none"> Zone types Delays Battery backup and power supply requirements Monitoring formats <ul style="list-style-type: none"> SIA and contact ID 4/2 and 3/1 Define types of peripherals and accessories <ul style="list-style-type: none"> Motion sensors Glass break detectors Smoke and fire Environmental sensors Vehicle detection Photo-electric beam devices Microwave beam devices Pressure sensors Sirens, strobes Security keypads Keyfobs Panic buttons Describe security infrastructure types <ul style="list-style-type: none"> Wired Identify access control devices and protocols <ul style="list-style-type: none"> Devices Protocols 	Unit 5, Topic B Unit 5, Topic D Unit 5, Topic B Unit 5, Topic D Unit 5, Topic B Unit 5, Topic D Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic A Unit 5, Topic B Unit 5, Topic B Unit 5, Topic B Unit 5, Topic B Unit 5, Topic B	A-2 A-2 A-2 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 A-1 B-1 B-1 B-3 B-3 B-3

Objective	Conceptual information	Supporting activities
4.3 — Identify, configure, install, maintain, and troubleshoot security and surveillance cameras.		
• Camera types	Unit 5, Topic C	C-1
– IP	Unit 5, Topic C	C-1
– Analog	Unit 5, Topic C	C-1
– Hybrid	Unit 5, Topic C	C-1
• Camera specifications	Unit 5, Topic C	C-1
– Lens type	Unit 5, Topic C	C-1
– Lux rating	Unit 5, Topic C	C-1
– Resolution	Unit 5, Topic C	C-1
– B&W vs. color	Unit 5, Topic C	C-1
– IP illumination	Unit 5, Topic C	C-1
– Power consumption	Unit 5, Topic C	C-1
• Camera applications	Unit 5, Topic C	C-2
– Indoor/outdoor	Unit 5, Topic C	C-2
– Day/night	Unit 5, Topic C	C-2
– Fixed vs. animated	Unit 5, Topic C	C-2
– Surveillance	Unit 5, Topic C	C-2
– Recording	Unit 5, Topic C	C-2
– Sequencing vs. multiplexing	Unit 5, Topic C	C-2

5.0 Home control and management

Objective	Conceptual information	Supporting activities
5.1 — Identify user interfaces and their appropriate applications.		
• Device types	Unit 6, Topic A	
– Remote controls	Unit 6, Topic A	
– Keypads	Unit 6, Topic A	
– Touchscreens	Unit 6, Topic A	
– Keyfobs	Unit 6, Topic A	
– Telephones	Unit 6, Topic A	
– Smartphones	Unit 6, Topic A	
– Cell phones	Unit 6, Topic A	
– PDAs	Unit 6, Topic A	
– Web tablets	Unit 6, Topic A	
– Personal computers	Unit 6, Topic A	A-2
– Laptops	Unit 6, Topic A	
• Describe the importance of simplicity and ease of use as it pertains to the end user	Unit 6, Topic A	
5.2 — Define and recognize control systems which integrate subsystems in the home. Describe their functionality, characteristics, and purpose.		
• Embedded control systems and Personal Computer (PC) based control systems	Unit 6, Topic A	A-1, A-2
– Compatibility and interoperability issues	Unit 6, Topic A	
5.3 — Identify commonly used communication protocols and their application.		
• IR	Unit 6, Topic A	A-3
• Serial	Unit 6, Topic A	A-3
• IP	Unit 6, Topic A	A-3
• RF	Unit 6, Topic A	
• Bluetooth	Unit 6, Topic A	A-3
• Contact closure	Unit 6, Topic A	
• Inputs (zones)	Unit 6, Topic A	
• Z-wave and Zigbee	Unit 6, Topic A	A-3
• ASCII	Unit 6, Topic A	A-3
• Proprietary protocols	Unit 6, Topic A	A-3

Objective	Conceptual information	Supporting activities
5.4 — Describe basic HVAC (Heating Ventilation and Air Conditioning) terminology and install peripheral devices.		
• Control layer	Unit 6, Topic B	B-1
– Compatibility	Unit 6, Topic B	
• Communication layer	Unit 6, Topic B	
– Compatibility	Unit 6, Topic B	
– IP based, wireless, serial, and proprietary	Unit 6, Topic B	
• Zones HVAC	Unit 6, Topic B	B-1
– Master slave configuration	Unit 6, Topic B	
– Microprocessor controlled configuration	Unit 6, Topic B	
• Programmable thermostats	Unit 6, Topic B	B-2
• Importance of referencing manufacturer specifications and compatibility	Unit 6, Topic B	
5.5 — Describe basic lighting terminology and install peripheral control devices.		
• Identify lighting control applications	Unit 6, Topic C	
– Indoor and outdoor	Unit 6, Topic C	
– Centralized and distributed	Unit 6, Topic C	
– Dimming	Unit 6, Topic C	C-2
– Scenes	Unit 6, Topic C	
– Relay/switching	Unit 6, Topic C	
– Occupancy/motion sensing	Unit 6, Topic C	C-1
– Time and event driven	Unit 6, Topic C	
– Window treatments	Unit 6, Topic C	
– Energy management	Unit 6, Topic C	
– Security interface	Unit 6, Topic C	
– Motor speed control	Unit 6, Topic C	
• Communication interface/bridge	Unit 6, Topic C	
– Power line phase couplers	Unit 6, Topic C	
• Identify lighting control protocols	Unit 6, Topic C	
– Z-wave	Unit 6, Topic C	
– Zigbee	Unit 6, Topic C	
– Powerline carrier (x10 protocol/PLC)	Unit 6, Topic C	
– UPB (Universal Powerline Bus)	Unit 6, Topic C	
• Proprietary RF and proprietary low voltage	Unit 6, Topic C	
– Recognize compatibility issues	Unit 6, Topic C	

Objective	Conceptual information	Supporting activities
5.6 — Identify and install component power protection devices.		
• Identify whole house protection options	Unit 6, Topic D	D-1
– Surge suppression	Unit 6, Topic D	D-1
– Power conditioning	Unit 6, Topic D	D-1
• Identify and install point protection	Unit 6, Topic D	D-2
– Surge protectors	Unit 6, Topic D	D-2
– UPS (Uninterruptible Power Supply)	Unit 6, Topic D	D-2
– Power conditioning	Unit 6, Topic D	D-2

6.0 Troubleshooting methodology and documentation

Objective	Conceptual information	Supporting activities
6.1 — Identify and apply the fundamentals of troubleshooting and diagnostics.		
<ul style="list-style-type: none"> • Use of testing equipment <ul style="list-style-type: none"> – Multimeter – Telephone buttset – Toner – Signal generation – Cable tester • Refer to prior documentation • Demonstrate when to communicate with technical support and what information is relevant • Troubleshoot common wireless interference issues 	Unit 7, Topic A Unit 7, Topic A Unit 7, Topic C Unit 7, Topic C Unit 7, Topic A Unit 7, Topic A Unit 7, Topic A Unit 7, Topic B	 A-1 C-3 C-3 A-2 B-1
6.2 — Given a scenario, demonstrate how to apply troubleshooting skills to integrated subsystems.		
<ul style="list-style-type: none"> • Networking • Audio/video • Telephony • Security • Home control 	Unit 7, Topic C Unit 7, Topic C Unit 7, Topic C Unit 7, Topic C Unit 7, Topic C	C-1 C-2 C-3 C-4 C-5
6.3 — List and describe the benefits of verification of installation.		
<ul style="list-style-type: none"> • Properly label wires • Wire mapping • Importance of documenting work upon completion <ul style="list-style-type: none"> – Input/output verification for all systems – Document wire placement • Certification of cable installation 	Unit 1, Topic D Unit 1, Topic D Unit 1, Topic D Unit 1, Topic D Unit 1, Topic D Unit 1, Topic D	D-1 D-1 D-1 D-1 D-1 D-1
6.4 — Deliver appropriate manuals and documentation to the end user upon completion of installation.		
<ul style="list-style-type: none"> • Select, archive, and appropriately distribute critical system information 	Unit 1, Topic D	D-2

PREVIEW

NOT FOR PRINTING OR INSTRUCTIONAL USE

Appendix B

CEA-CompTIA DHTI+ acronyms

This appendix covers these additional topics:

- A** Acronyms appearing on the CEA-CompTIA DHTI+ exam.

Topic A: Acronyms list

Explanation

The following is a list of acronyms that appear on the CEA-CompTIA DHTI+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

Copyright © 2006 by the Computing Technology Industry Association. All rights reserved.

Acronym	Spelled out
PC	Personal Computer
DHCP	Dynamic Host Configuration Protocol
ASCII	American Standard Code for Information Interchange
ATSC	Advanced Televisions Standards Committee
BC	Bare Copper
BNC	British Naval Connector
CAT5	Category 5
CATV	Community Antenna TV/ Cable Television
CCS	Copper Clad Steel
COAX	Coaxial
CRT	Cathode Ray Tube
dB	Decibel
DD	Dolby Digital TM
DDEX	Digital Data Exchange
DLP	Digital Light Processing TM
DNS	Domain Name Service
DRM	Digital Rights Management
DSL	Digital Subscriber Link
DTS	Digital Theater Sound
DTSES	Digital Theater Sound -Extended Surround
DVB-S	Digital Video Broadcasting Satellite
DVB-T	Digital Video Broadcasting Terrestrial

Acronym	Spelled out
DVD	Digital Versatile Disc
DVDA	Digital Versatile Disc Audio
DVI	Digital Visual Interface
DVR	Digital Video Recorder
HDMI	High Definition Multimedia Interface TM
HVAC	Heating Ventilation Air Conditioning
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	Infrared
LAN	Local Area Network
LCD	Liquid Crystal Display
LCoS	Liquid Crystal on Silicon
LNB	Low Noise Block Down Converter
MAC	Medium Access Control
MP3	Motion Picture Standards Group Layer 3
MRAV	Multi-Room Audio Video
NAS	Network Attached Storage
NTSC	National Televisions Standards Committee
PAL	Phase Alternative Line
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PLC	Powerline carrier
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QS	Quad Shield

Acronym	Spelled out
RCA	The Radio Corporation of America™
REN	Ringer Equivalence Number
RF	Radio Frequency
RGB	Red Green Blue
SACD	Super Audio Compact Disc
SIA	Security Industry Association
SSID	Security Set Identifier
STP	Shielded Twisted Pair
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	Universal Datagram Protocol
UPB	Universal Powerline Bus
UPS	Uninterruptible power supply
UTP	Unshielded twisted pair
VoIP	Voice over IP
VSB	Vestigial Side Band
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2

Course summary

This summary contains information to help you bring the course to a successful conclusion. Using this information, you will be able to:

- A** Use the summary text to reinforce what students have learned in class.
- B** Direct students to the next courses in this series (if any), and to any other resources that might help students continue to learn about CEA-CompTIA DHTI+.

Topic A: Course summary

At the end of the class, use the following summary text to reinforce what students have learned. It is intended not as a script, but rather as a starting point.

Unit summaries

Unit 1

In this unit, students identified features, functions, and benefits of **DHTI systems**. Next, they identified the basic components of DHTI systems. Students also examined the information needed by technicians to design and install DHTI systems. Finally, they discussed the benefits of installation verification and ways to deliver manuals and documentation to the users.

Unit 2

In this unit, students worked with **computer networks**. First, they configured a **LAN connection** and joined a **workgroup**. They then used their network connection to **share file and printer resources** on the network. Students also learned how to create an **Internet connection** and examined **WAN bandwidth technologies**. Finally, they examined methods to implement **network protection strategies** including **Windows Firewall configuration** and **wireless network security** methods.

Unit 3

In this unit, students learned about **audio and video system** concepts. First, they examined **home theater system components and characteristics**. Then, they learned about **content management systems** and discussed how they are used in home theater systems. Finally, they set up and configured audio and video systems and examined **multi-room A/V systems and standards**.

Unit 4

In this unit, students learned about telephony and VoIP services. First, they learned that **POTS**, an **analog voice telephone** system, can transmit data at up to 56 Kbps, about the wiring standards, and the common issues affecting POTS connections. Next, students learned about **digital telephone communication** systems and **VoIP** features as well as **QoS** issues affecting VoIP connections. Finally, students learned about telephone systems, including **PBX** and **key systems** as well as **voice messaging** and **unified messaging** systems.

Unit 5

In this unit, students learned about **security and surveillance systems**. First, they learned basic **security terminology** and about types of **security peripherals and accessories**. Then they examined wired and wireless security infrastructures and examined **access control devices**. Next, students examined features of cameras and then discussed how to configure, install, maintain, and troubleshoot **security and surveillance cameras**. Finally, students installed and configured **security system components**, including the **security panel**, and interior, exterior, and environmental components.

Unit 6

In this unit, students learned about **home control and management** systems. First, they examined methods used to integrate control subsystems, including **PC-based control systems**, and **ZigBee**, **Z-Wave**, and other protocols. Next, students identified basic **HVAC** terminology and configured **HVAC control devices**. They also learned basic lighting terminology and installed **lighting control devices**. Finally, students examined and installed component and whole-house **power protection devices**.

Unit 7

In this unit, students learned about **troubleshooting DHTI systems**. First, they examined various **troubleshooting and diagnostic tools and methods**. Next, they learned to **troubleshoot wireless interference issues** for both wireless computer networks and home control systems. Finally, they applied **troubleshooting** skills to integrated subsystems, including **wired computer network**, **A/V subsystems**, **telephone subsystems**, **security systems**, and **home control systems**.

Topic B: Continued learning after class

Point out to your students that it is impossible to learn to use any software effectively in a single day. To get the most out of this class, students should begin working with DHTI to perform real tasks as soon as possible. Course Technology also offers resources for continued learning.

Next courses in this series

This is the only course in this series.

Other resources

For more information, visit www.course.com.

Glossary

802.1x

Protocol is a mechanism to authenticate wireless users. It is a port-based, authentication framework for access to Ethernet networks.

AC cable

Armored cable; a type of cable sheathed in metal. Also, any cable used for AC wiring.

AC power

Alternating current electric power; the standard electric service in homes.

Access control

Restriction on who has the right to use a computer system or to enter a physical location.

Access point

A wireless hub or device through which a wireless node can connect to a LAN. It is a device that functions as a transparent bridge between the wireless clients and the existing wired network

Active crossover

Frequency divider at the line level.

Active Directory

A centralized system that controls computer and user configuration settings, security settings, and access to resources on a LAN.

Adaptors

Devices that change audio and video connectors from one form to another, including gender changes.

Administrator

A person designated to maintain and control a computer system or subsystem.

ADSL splitter

A device attached to the NID that splits an incoming ADSL data line, isolates other telephone lines and equipment, and allows a home run to be installed to the modem.

Advanced Television Systems Committee (ATSC)

The government-run and industry-influenced group that sets standards for the television industry.

Air conditioning (A/C)

The part of an HVAC system that provides cool air to lower the indoor air temperature.

Air handlers

The mechanical devices that move air in an HVAC system. They are mainly blowers and fans.

Alarm

An audible warning of fire, illegal entry, or other security breach. Usually a siren, bell ringing, or similar sound.

Alternating current (AC)

The type of power that almost all homes receive from the electric utility company.

Alwayslive duplex outlets

An AC electrical outlet that is not controlled by a switch and always has current available.

American Wire Gage (AWG)

The standard for electrical wire sizes.

Ammeter

A device specifically made for measuring current.

Amperes

The unit used to measure electric current flow.

Amplifier

A device that strengthens the power of an RF signal it receives from an antenna or pre-amplifier.

Amplitude modulation (AM)

A method of converting sound waves to radio signals by varying the amplitude (strength) of the signal, but not its frequency.

Analog

Sound or video signals that are analogous to (have patterns similar to) the actual sounds or images.

Analog data

Data in nonnumeric form such as radio waves, sound waves, and so on.

Antenna

The component of a radio or television receiver that receives a broadcast signal from a distant transmitter.

AppleTalk

The Mac OS uses a suite of networking protocols called AppleTalk but also supports the networking protocol suite TCP/IP.

Appliance

Any piece of equipment that performs a specified task.

Arm

To activate a security system so that its sensors are functioning.

Aspect ratio

The ratio of a video screen's width to its height. NTSC screens have a 4:3 ratio; HDTV screens a 16:9 ratio.

Atrium

An area within a home that is open to the outside or walled in glass, in which plants can grow as in the outside yard.

Attenuation

Weakened by distance from the source; resistance; used to describe radio and television signals.

Automated control

A method for controlling HVAC systems by preset programming rather than manual setting of controls.

Automated doors

Doors mechanized to open and close on command by means of cable pulls or hydraulic actuators.

Automated furniture

Any piece of furniture that can be remotely directed to open, move a display or object within it into a functional position, or change its own configuration by mechanical means.

Automated lift

Any mechanical system designed to lift people or objects from a lower position to a higher level.

Automatic Private IP Addressing

Windows 2000 and Windows XP computers can assign themselves IP addresses by using Automatic Private IP Addressing (APIPA). They assign themselves IP addresses in the range of 169.254.0.0 to 169.254.255.255, if they haven't been assigned an IP address manually

Automation

Performing a task or function by means of a programmed device or system without the need for human supervision.

Automation

The process of controlling a lighting or other system remotely, either with manual commands from a controller or by a programmed set of instructions from a computer.

Average use

The amount of electricity used in a home over a period of time, usually a day.

Balun

A transformer that enables you to send a signal of one impedance over a cable that requires different impedance. Used in pairs.

Bandwidth

The amount of data that can travel over a communication line or wireless connection in a given length of time.

Baud

One complete cycle or wave in an analog transmission signal. A baud starts at zero voltage, goes up to maximum positive voltage, comes back to zero, goes to maximum negative voltage, and finally returns to zero voltage.

Biometric identifiers

Unique distinguishing physical features of an individual that can be used as means of identification. They include fingerprints, retinas, voice, and facial characteristics.

Blower

A device that uses a rotating bladed wheel to move air in an HVAC system. Not the same thing as a fan.

Bluetooth

A short range (100 meters), wireless connection technology now being used for networking.

Boiler

A device for heating water to be used for heating a building. Not the same as a water heater.

Break switch

A sensor that monitors a closed switch and signals if the switch is opened and the circuit broken. Used on doors, windows, and containers that should remain closed as their normal state.

Breaker

A safety device that is wired into a circuit to cut off current flow if the circuit becomes overloaded.

Bridge

An intelligent switch that limits data flow on a LAN.

Broadband

Any method of transmitting large amounts of data in a short time span. Usually accomplished by using multiple frequencies or data streams; a large (or wide) bandwidth technology.

Bus topology

One form of network architecture for Ethernet.

Bypass

Any means of evading a security device by making it appear to be functioning in a normal state when, in fact, conditions have changed. A window sensor, for example could be bypassed by slipping a loose plate onto its contact points to make the switch continue to signal normal (closed) even when the window is opened.

Bypassed

In security systems, a situation where a sensor is made to appear in normal status, but in reality is not.

CableCard

A card from the cable company that plugs into a computer or directly into a TV to descramble encrypted signals from the provider.

Cable modem

A device that converts digital data to analog signals and connects a LAN to an ISP via the cable television connection.

Cable pull

A motor-driven mechanism that uses a looped cable to move an object horizontally or vertically.

Cable run

A cable installed between two connecting points such as a patch panel and jack.

Call restriction

A telephone system feature that allows certain calls to be blocked from incoming or outgoing lines.

Caller ID

A system in which a signal sent by the telephone company with an incoming call identifies the calling number and its registered owner. Telephones with electronics capable of reading this signal display the caller ID information on a small LCD screen.

Camera

A device that creates a video image in digital or analog form. Cameras can produce still images or moving images.

Carrier frequency

In radio transmission, a signal at high frequency on which a signal of lower frequency is carried.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

A method of data transmission in which nodes avoid data packet collisions through use of a token or other device controlling the movement of data.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

A method of data transmission in which data packets contend for space on the network, and nodes sense packet collisions that require resending.

Category 2 telephone wire

A low-speed data wire containing two pairs of solid core insulated wires. Named for its widespread use in wiring analog telephone lines.

Category 3 wire

A low-speed data wire with the same composition as Category 2 wire but having either four or six pairs of wires.

Category 5 (Cat5) cable

A high-speed eight-wire UTP data cable for Ethernet.

Cathode ray tube (CRT)

A monitor or TV screen.

CatX cable stripper

A tool for cutting and removing the outer jacket from Category 5 and other similar types of cable.

CD burner

A device for recording compact discs (CDs). A CD burner can also play a CD, but CD players are not always burners.

CD player

A device for playing recorded compact discs.

CDR (CDRecordable format)

A compact disc that can be recorded once on a CD burner, but is then a permanently fixed recording that cannot be changed.

CDRW (CDRewritable format)

A CD that can be recorded multiple times with succeeding recordings added to or replacing older ones on the disc.

Central heating system

The part of an HVAC system that provides warm air from a central furnace to raise the indoor air temperature.

Central processor

The main computer in an HTI system or, alternately, the component in a computer that performs calculations on data.

Centrex

Central exchange, the main switching point in the telephone company where calls are connected by switching them to the line called.

Certification

The process of attesting to the qualification or competence of a person to perform certain services.

Checksum

A mathematical method for a receiver to determine if a data packet has been corrupted.

Cipher lock

A door lock that opens only when a numeric code is entered on a keypad mounted near it. The code can also be placed on a memory card that is swiped through a reader to open the lock.

Circuit

A conducting “circle” in which electricity flows from a source to a device, through the device, and back to the source.

Circuit switched lines

The normal method of completing an analog call in which the calling line is physically connected to the called line by a defined path, and the path is kept open for the duration of the call.

Circulating pump

A device in a radiant heating system that continuously circulates the heated water through the boiler and heating pipes.

Clean power

AC current that does not contain noise, interference, surges, or spikes.

Cliff effect

A description of the sudden termination of the range of digital video transmissions that can end as if they “fell off a cliff.”

Codec

Coding/decoding: a software program or hardware device that encodes and/or decodes digital transmissions.

Command module

An X10 technology controller that sends commands (manually generated or programmed) to control modules that control lights.

Compact disc (CD)

A plastic disc on which audio files are encoded using the pulse code modulation method.

Compression

Any technique that uses math algorithms to reduce the size of digital files for storage or transmission.

Compressor

The part of an A/C system that squeezes the refrigeration gas under pressure into a smaller volume until it converts into a liquid.

CompTIA

Computer Technology Industry Association, a global information technology (IT) trade association with more than 13,000 members in 89 countries. It works to advance the IT industry, promote IT public policy, and develop standards for training of professionals in the industry.

Concealed enclosure

A box or other three-dimensional shape built behind a wall or other flat surface to contain an object normally hidden from view.

Concealed wiring

Retrofitted wiring installed within the finished walls of a structure.

Condensation

The process in an A/C system by which the refrigeration gas changes back into a liquid under pressure. Also, the process by which water vapor is removed from cooled air and is deposited as a liquid.

Condenser coil

A coil through which hot refrigerant passes and is cooled by flowing air in the same manner as an automobile radiator cools engine coolant.

Condensing unit

The part of an A/C system in which the refrigerant is converted back into a liquid from a gaseous state.

Cone

The part of a speaker that vibrates in the air, producing sound.

Contact ID

A security monitoring format.

Control device

Any device that initiates a process, directs equipment to perform a function, or responds in a preset manner to remote commands.

Control module

In X10 systems, any of the devices that receive lighting control instructions from the controller and implement them by adjusting the lights.

Controller

The electronic device that controls the operation of sprinkler system zone valves through a preset, timed schedule.

Controllers

Lighting control devices that send lighting commands to control modules in an automated lighting system.

Converter

A device that changes digital signals into analog, or vice versa.

Converter

A device that renders digital data into analog signals in audio and video systems.

Cooling coil

The part of an A/C system that cools the surrounding air by the expansion of the refrigerant in the coil, which absorbs heat from the air.

Cordless phones

Phones with transceivers (transmitters and receivers) that operate on radio frequencies. They have a limited range from the base unit, which contains another transceiver.

Counterweight

A heavy weight suspended on a cable or chain looped over a support wheel. The cable connects the counterweight to the object whose weight it is balancing. When the balanced object moves in one direction, the counterweight moves in the other.

Credential

A written certification that an individual has specified qualifications, abilities, or expertise.

Crossover

In speakers, crossover sends frequency ranges to the appropriate speakers.

Crossover network

A wiring circuit in speaker systems that permits several speakers of different ranges to function seamlessly together.

Crown molding

Angled decorative slats installed at the junction of interior walls and ceiling. It can conceal cable.

Current

The flow of electricity, measured in amps.

Daisy chain wiring

Wiring light fixtures in parallel to one another with only the first light being connected directly to a power supply and each of the others receiving power in succession down the chain.

Dampers

Devices that act like doors in ducts. They can be closed to block air passage or opened to allow it.

Decibel (dB)

A unit for measuring sound level. Used in audio engineering.

Decoder

A device for rendering data received in an encrypted form into a form that can be used by a computer or displayed by a video or audio system.

Demarcation point

The physical place where the incoming telephone lines from the telephone company connect to the internal wiring of the home; also known as demarc.

Detection devices

Sensors that discern changes in conditions that indicate the presence or passage of a person or persons.

Detector

A sensor that is designed to react to a certain event such as pressure, motion, heat, or light.

DHCP server

A server on which the network service is hosted.

Dial tone

A continuous tone sent on a telephone line by the PBX or the central exchange to indicate that it is available for a call.

Digital

Any kind of data that is recorded in numerical (discrete) form rather than analog (continuously varying).

Digital audio file

A recorded music or voice audio segment stored on a computer hard drive or other similar media.

Digital audio tape (DAT)

Standard for recording uncompressed digital audio on tape at the same quality level as a CD.

Digital cable ready

A government designation for television sets denoting their capability to play digital cable programs.

Digital data

Data in the form used by computers and that consists only of the binary numeric digits 1 and 0. Nearly all forms of information can be rendered into digital form for processing or transmission and then rendered back into a form that can be displayed or understood by people.

DHTI

Digital Home Technology Integration is the concept of a connected home environment in which a central computer system, programmed or otherwise directed by the homeowner, manages and distributes incoming and outgoing Internet and audiovisual digital data, and controls the network, appliances, security, and utilities of the home.

Digital Rights Management (DRM)

The technologies are used to control both use and access of digital content and the hardware on which the content is accessed. It also refers to the restrictions placed on a specific piece of digital content.

Digital Subscriber Line (DSL)

A telephone line used for high-speed digital data and voice transmission and is always available for the subscribing user's exclusive use.

Digital television (DTV)

Television signals that are in numerical format and create a picture in pixels rather than rasters as does analog TV.

Digital video discs (DVDs)

Media for recording digital video.

Digital video/audio switcher

A device that receives digital signals from multiple sources and routes them as instructed to multiple outputs.

Direct Sequence Spread Spectrum (DSSS)

A method of signal hopping or rapidly changing frequencies in a specified sequence to transfer data at high speed.

Disarm

Deactivate a security system so its sensors are not functioning.

Dish antenna

A parabolic-shaped antenna that receives satellite broadcasts.

Distortion

Changes in reproduced sound waves caused by excessive power or other interference in the recording and playback processes.

Distribution

The process of transmitting data throughout a system so that it is available to all components.

DLP

Digital light processor. A front projection TV system that uses an array of mirrors for each pixel.

DNS server

Special computers on the Internet that keep databases of IP addresses and their corresponding domain names.

DNS suffix

DNS host names include a NetBIOS-type computer name plus the DNS suffix of the DNS domain of which the computer is a member.

Domain controller

A server with a central database of user accounts that are used to authenticate users.

Domain name

A unique name assigned to a network and registered with ICANN.

Domain Name Service (DNS)

A part of the TCP/IP protocol that translates domain names into their corresponding IP addresses.

Door strike

An electronically controlled door strike plate that allows the door to be unlocked by an electronic signal.

Dot matrix printer

A printer that prints using a matrix of small pins that strike the paper through a ribbon and combine to form characters.

Dot pitch

The distance between the colored phosphor dots in a color monitor that determine the sharpness of its image.

Double protection

In security systems, at least two devices monitoring a means of entry into a home so that if one is disabled or fails, the other still detects any intruder.

Downlink

Digital data being transferred into a ground-based system from a satellite.

Drape pull mechanism

A device for opening or closing drapes or blinds by means of a motorized loop cord.

Drip irrigation system

A type of irrigation system in which small tubes deliver water flow directly to individual plants or plots of ground without spraying. The system conserves water compared to spraying sprinkler systems.

Drive ring

A metal ring that can be hammered into walls to carry cable on the exterior of buildings.

Drop-down mechanism

A mechanical device that lowers a display or piece of equipment from a concealed overhead position to a level where it can be seen or used.

Drywall

The paper-covered gypsum board that is fastened to studs to finish the walls in most homes.

Duct

A metal tube or open ended box through which air can flow. Can be rigid or flexible and of any size.

Dumbwaiter

A small elevator designed to carry objects from one floor to another in a building. It is electrically powered and moves up and down on rails in an open shaft.

Duress code

An access code (to be used in the event a person is accosted or threatened at the door) that opens the door and summons help.

DVB

The standards define a suite of open standards for digital video broadcasting. Separate standards for cable, terrestrial, and satellite communications.

DVD

Digital video disc. A small plastic record on which digital video programs are recorded using a laser process.

DVDA

DVD-Audio. DVD discs that contain special audio tracks that can be played only on DVD-Audio players.

Dynamic Host Configuration Protocol (DHCP)

A method of automatically assigning IP addresses to nodes on a LAN.

Eave

The underside of a roof that overlaps the outer walls of a building.

Electric service

Electric power purchased from a utility, also the cable bringing the electricity to a home from the utility.

Electromagnet

A magnet created by passing a current through a coil of wire. Used in audio speakers and many other devices.

Electromagnetic field

Force field of electrons generated by high-voltage equipment and wires.

Electronic deadbolt

A deadbolt lock that can be opened or closed via an electronic signal from the alarm system.

Embedded control system

A device that contains only the computer functions needed by the device.

Emergency response

Any assistance delivered as a result of a security system call-in. Fire department, police department, and medical teams are all emergency responses.

Encoder

A device or software program for changing analog audio or video signals into digital format. Video versions are also called coders.

Enhanced Definition Television (EDTV)

An ATSC-defined television that can play both analog and SDTV digital programs.

Equalizer

An audio device for balancing the levels at which sound frequencies are recorded or played back.

Ethernet

The most common form of LAN architecture. It uses bus or star topology and employs CSMA/CD to manage the flow of data on the network.

Evaporative or “swamp” cooler

A type of air cooler that works by evaporation of water into air, which is thereby cooled as it passes through the cooler.

Extensions

In telephone systems, an additional phone wired in parallel into a single line.

Face plate

The decorative cover on wall boxes that contain data jacks or AC power outlets.

Failsafe

A theoretical term for a security system that can't be disabled or bypassed. Not possible to achieve in actual systems.

False alarms

Any security breach not produced by a genuine security threat.

Fan

A device consisting of a balanced set of angled blades on a shaft spun by a motor. Fans move air and are one type of air handler.

Fax machines

A digital device that operates on an analog telephone line. It sends and receives printed documents by transmitting them as bit-mapped images.

Fiber Distributed Data Interface (FDDI)

Large, fast networks that are constructed almost entirely using fiber optic cable.

Fiber optic cable

A very high-speed means of transmitting data by using light beams through glass or plastic threads or fibers.

Field

One scan of an interlaced television frame that refreshes one half the frame.

Filter

A device to remove interference from an electric circuit.

Fireplace igniter

An electric device that lights a gas-fired fireplace by producing a spark near the gas jet, which ignites the natural gas.

Firestop

A wooden crosspiece set between studs in interior walls to retard fire.

Firewall

Hardware or software that controls the data entering or leaving a computer system. Used to maintain the security of the system.

FireWire

A 1394 standard data connection for transmitting digital data at high speed between two devices or nodes on a network.

Flat panel screen

An LCD monitor or television.

Flow meter

A device that measures the amount of water flowing in a pipe and signals its measurement to a recording device. Used to detect leaks or breaks in pipes or sprinkling systems.

Flow valve

A type of valve that measures the amount of water flowing through it and can adjust that flow automatically.

Fluorescent lighting

Lighting tubes that contain phosphorescent material and glow when a high-voltage current is passed through them. Made in various lengths up to 8 feet.

Forced air

A type of heating or A/C system that works by blowing heated or cooled air into a home through ducts and air vents.

Frame

One complete refresh of a television screen, which can be two scans (fields) if interlaced and one scan if progressive.

Freeze sensor

A device that sends a signal when the temperature around it falls to near the freezing point of water (37 degrees normally, although some can be set to lower or higher temperatures) so that action can be taken to prevent freezing.

Frequency division multiplexing

An analog technology for carrying multiple data streams, voice, or data on the same wires.

Frequency Hopping Spread Spectrum (FHSS)

A method of signal hopping or rapidly changing frequencies in a random sequence to transfer data at high speed.

Frequency modulation (FM)

A method of broadcasting sound by varying the frequency of the carrier wave, but not its strength.

Furnace

A device for heating air so that it can be blown into the interior of a home.

Gas detector

A device that senses the presence of natural gas, carbon monoxide, or other poisonous gas.

Geared rack

A flat strip of metal geared on one side. It is mounted in a stationary position and a powered gear wheel travels along it in either direction, pulling whatever is attached to the gear.

Ground

A wire that connects an electric device to the earth so that excess current can flow to the ground rather than elsewhere.

Ground start system

Local telephone system that seizes a telephone line as soon as a receiver is lifted so that no other call can transmit on the line.

HDTV tuner

A digital television tuner that receives full resolution HDTV signals in 16:9 format.

Header

Data at the beginning of a data packet identifying its source and destination.

Heat sink

A relatively large piece of metal or other material placed near a heat source to absorb heat from it and dissipate it into the surrounding air.

Heat transfer

The process by which heat radiates from warmer objects to cooler ones.

Heating cable

An electric cord that has high resistance to electricity and gets hot when current passes through it. Used to warm pipes, rain gutters, and other areas so they don't freeze.

Heating, ventilation, and air conditioning systems (HVAC)

A specialized field in the construction industry that installs and maintains the equipment and infrastructure of these systems.

High definition television (HDTV)

Digital television format with a 16:9 aspect ratio and high resolution.

Home lighting system

The entire electrical light configuration in a home, including all interior and exterior lights and the controls (manual or automated) that direct them.

Home run cable

A data cable running directly from an ADSL splitter to the network modem, ensuring a clean incoming signal.

Home run connection

A wired connection that links a light directly to its power supply without the current to it passing through any other fixture except a switch.

Home security system

An HTI subsystem of hardware and software designed to prevent unauthorized persons from entering a home or yard, using any of its data systems, or removing anything from them.

Home Technology Integration (HTI)

A connected home environment in which a computer system manages data and controls subsystems in the home.

Home theater

An HTI subsystem for displaying television programs and recorded video programs. Similar to a home entertainment center, but usually specialized primarily for video viewing.

HomePNA

Dominant standard of HomePNA technology currently in use for networks using telephone lines for connectivity.

HomeRF (Home Radio Frequency)

A wireless network technology for home LANs.

Host

Another name for a computer on a LAN.

Hot wire

The wire in a cable that is connected to the source of electric potential, usually colored black.

HPNA 2.0

Network standard currently in use for HPNA networks.

Hub

A device that connects nodes on a LAN and broadcasts data received from any node to all other nodes.

Huffyuv

A lossless codec for digital video compression.

Humidifier

A device that adds moisture to an incoming air stream.

Humidity

Moisture contained in air. All air contains some water vapor (gaseous water). The amount can vary with pressure and temperature of the air.

Humidity detector

A device that measures the amount of moisture in the air around it and signals that data to a controller or computer.

Hydraulic cylinder

A device that uses oil under high pressure to force a piston rod out of a cylinder. The moving rod lifts whatever is attached to its other end.

IAX

VoIP protocol that makes use of port 4569.

IEEE

Institute of Electronic and Electric Engineers. Organization that develops computing and telecommunication standards such as those for LANs.

IEEE 1394

A fast serial protocol running from 100 to 400 Mbps.

IEEE 802.11b

WiFi version of the IEEE 802.11 wireless network standard.

IEEE 802.11g

New and extremely fast version of IEEE 802.11 standard not yet in use.

Inclined ramp

A sloped walkway used in place of stairs. It can be traversed by wheeled vehicles as well as on foot.

Infrared (IR)

Technology that sends command signals using infrared light, which is invisible to human eyes.

Infrared devices

A device that functions by detecting heat (infrared-wavelength energy) or changes in the heat level of its surroundings.

Infrastructure

Any of the wiring, conduit, connectors, wireless hubs, switches, routers, and other hardware that enable the subsystems of an HTI system to communicate with one another and the outside world.

Inside arming

Code or command that activates perimeter devices in the security system and may activate some interior devices, but usually not all. Inside armed is the normal status for the security system at night while the family is asleep.

Integrated Services Digital Network (ISDN)

A technology that uses a telephone line to transmit digital data at high speed.

Intercom

A line in key systems that allows any extension to connect to any other for an internal call without accessing an outside line.

Interference

Noise and conflicting signals that can occur in transmissions in unlicensed radio bands such as the ISM band.

Interference

Any signal that corrupts or blocks a data signal.

Interlaced

Method of refreshing a video screen in which only odd-numbered lines are scanned on one pass and even-numbered lines on the next.

Internet

A worldwide web of interconnected but independent networks over which data travels from source to destination by various routes.

Internet Corporation for Assigned Names and Numbers (ICANN)

The group that assigns and regulates domain names and IP addresses through accredited registrars.

Internet Home Alliance (IHA)

An industry group whose objective is to develop the market for home technologies that require a broadband or persistent connection to the Internet.

Internet service provider (ISP)

A company that provides Internet connections to home and business LANs.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

The protocol used by Novell NetWare networks.

Inoculation

The process of calculating and recording checksums to protect against viruses and worms.

Intranet

Internal company or home Internet-like network maintained for the benefit of employees or residents.

Intruders

Any unauthorized person trying to enter a secured home or yard.

IP address

Internet Protocol address, a 32-bit address consisting of four numbers separated by periods, used to uniquely identify a device on a network.

IP camera

A digital camera that is directly connected to the network.

IPCONFIG

TCP/IP utility that displays the computer's adapter address, IP address, subnet mask, and default gateway, and allows the DHCP to be renewed or released by the user.

IR illumination

In surveillance cameras, a method of lighting an area instead of using flood lights or a flash.

Jack

A connecting device terminating a cable into which a plug is mated to connect a node.

Joist

A horizontal support beam in a floor.

Key system

A local telephone system in which multiple phones are connected to multiple lines by switching buttons so that any telephone can use any line.

Keyboard

An alphanumeric data input device for a computer. It may contain additional keys that input specific commands or run sequences of data.

Keypad

A numeric pad similar to a telephone dial pad that is used to input passwords to cipher locks and other security devices.

Laser light

Coherent light waves transmitted in parallel beams so that they maintain their intensity over long distances. Used in light beam sensors and many other devices.

Laser printer

A printer that works by picking up toner on a charged image on the surface of a rotating drum and depositing it on paper where the image is fused in place.

Latchkey function

A command or code that programs the call-in device to notify a set telephone number when a specific door of the home is opened during set hours.

LCoS

Liquid Crystal on Silicon. A projection system that has been reduced to an LCD system on a chip.

Leased

The IP address is assigned or leased to the computer for a specified duration—anywhere from a few hours to a few days, depending on how the DHCP server is configured by the network administrator.

Light beam sensor

A device in two pieces, one of which transmits a beam of light to the other across a distance. If the light beam is obstructed, the sensor signals its failure to arrive.

Light scenes

Illuminated rooms or areas within a room that not only provide light but beautify a setting or invoke a mood.

Light sensor

A device that senses the presence of light and signals it or senses the absence of the light and signals it.

Light emitting diode (LED)

An electronic device, similar to a vacuum tube, that emits red light or infrared radiation.

Line level

The signals between components before amplification are line-level signals.

Line of sight

A term used to describe the location of wireless transmitters and receivers. It means that the receiver must be visible when viewed from the transmitter for the signal to be received.

Line seizure devices

Disconnects any connection already made on a phone line in order to place an emergency call through the security system dialer.

Line speed

The amount of data that can travel over a communication line or wireless connection in a given length of time.

Liquid crystal display (LCD)

A thin, lightweight type of video display that uses liquid crystal material sandwiched between two layers of electrodes to create a color image.

Load

The amount of current flowing in a circuit, measured in amps or watts.

Local area network (LAN)

A regionally confined network consisting of computers that communicate and share data and services.

Lockdown feature

A program in some security systems that allows all door locks to be deactivated during specified times so that they can't be opened from the outside at all, even with a valid access code.

Loop pull cord

A continuous cord that extends through a drapery rod, or blind and is used to pull the drape or blind open or closed. The cord forms an open loop on one end of the rod or frame.

Loop start system

Local telephone system in which a Centrex-supplied dial tone indicates when a line is available for a call, but no line is seized until a call is actually placed.

Lossless

Type of video compression in which no data is lost. Huffvuv is an example.

Lossy

Type of video compression in which some data is lost, but files can be made smaller than with lossless compression.

Lux

A measurement of the amount of light that falls on an object.

Lux rating

A subjective measure that describes how much light is required for an acceptable image to be captured by the camera.

Macros

Sequences of commands in a specified order that a programmable device stores in memory and executes at preset intervals.

Magnetic key

A key similar to a plastic credit card with its access information coded on a magnetic stripe that can be read by an access device.

Magnetic media

Any media with a ferrous coating capable of storing analog or digital data recorded on it by a magnetic head.

Magnetic recording

Any analog or digital data recorded on magnetic media.

Magnetic tape

Plastic tape coated with ferrous material for recording data.

Make switch

A sensor that monitors a switch that should remain open and signals if it is closed. Most commonly used as pressure pads that are closed by weight passing over them.

Matrixed channels

Output channels that are derived electronically from input channels.

MC cable

Metal-clad cable used for AC wiring.

Mechanical relay

An electrical device activated by an electromagnet being energized that functions as a switch to turn a control current on or off; an automatic, remote-controllable switch.

Media

Any means of storing or recording audio or video information: magnetic tape, CD, DVD, and phonograph record are examples.

Microphone

A device that converts sound waves into digital or analog data, which can be transmitted over distances and replayed or stored.

MIDI (Musical Instrument Digital Interface) file

A type of digital music recording in which the file stores an actual musical score. MIDI files can be played on any electronic instrument or software-equipped computer.

MiniDV cassettes

A small-format recording medium used in many digital video cameras.

Modem

An electronic device that converts digital data into a form that can be sent over a telephone line. Modems are the most common method of connecting a home computer to the Internet through a telephone line to a service provider.

Monaural

Having only one track or sequence; not stereo. Used to describe single-track audio recording.

Monitor

A device for displaying data in text or picture (graphic) form. Also, a sensor that monitors one or more environmental conditions.

Monitored

In security systems, watched either by a person at a control console or by the electronic security panel itself, so that any change in status can be responded to.

Monitoring service

A commercial service in which a company's staff continually watches a home security system via a telephone line linked to the home.

Motion sensor

A device that detects any object that radiates heat moving into its range and signals the change in its surroundings.

Motorized drive

A mechanical device that uses an electric motor and gear assembly to power a piece of equipment to perform a specific function.

MP3 file

A file created with an audio compression algorithm with the same name.

MP3PRO

A file created with an audio compression algorithm with the same name; higher compression than MP3, but equal in quality.

MPEG1

A file created with a video compression algorithm of the same name.

MPEG2

Video compression algorithm used for DVD video recording.

MRAV

Multi-Room Audio Video standard for adding distributed audio and video in the home environment. Defined by CEA.

Multimeter

A meter that is used to measure multiple electrical properties.

Multiplexing

Combining different types of data from multiple sources on a single transmission path.

Multistation Access Unit (MAU)

Device used in a token ring star design to which all nodes are connected.

Multisystem VCR

A video player capable of playing NTSC, PAL, or SECAM video cassettes on any analog television.

Name resolution

The process of translating a familiar name into an IP address.

Narrow band

In telecommunications systems, bandwidth of 128 Kbps or less.

National Electric Code (NEC)

A safety standard for electrical wiring and installation developed by the NFPA.

National Fire Protection Association (NFPA)

Publisher of the National Electric Code.

Network

A group of computers, information sources, and peripheral devices connected by cable or radio so that they can share data and communicate with one another.

Network Attached Storage (NAS) device

A storage device containing an embedded operating system and attaches directly to the network rather than to a computer.

Network BIOS Extended User Interface (NetBEUI)

A Microsoft proprietary protocol commonly used for LANs.

Network interface card (NIC)

A device for connecting a node to a LAN.

Network interface device (NID)

A device that connects the ISP service line to a home's inside telephone and data wiring.

Network operating system (NOS)

Manages LAN resources.

Network printer

A printer of any type connected to a LAN as a node with its own IP address.

NM cable

Nonmetallic cable used for AC wiring.

Node

A computer or other device connected to a LAN by a NIC.

Non-interlaced

A type of screen refresh that renews each line of the screen in order. This method of refreshing is also called progressive.

NTSC format

Standard analog U.S. TV format with 525 scan lines and 4:3 aspect ratio.

Numeric code

A group of digits that serves as a password and must be entered into a cipher lock to open it.

Obstruction detector

A safety device that detects anything unusual under a descending garage door and stops the door's downward movement.

Off-the-shelf hardware

Mechanical assemblies already designed and built to accomplish movements in automated furniture or assist in the construction of custom systems.

Ogg Vorbis (OGG)

An open source video compression format and hence free of any patents.

Ohm's law

Describes the relationship among amperes (amps), or the amount of current flowing, volts, which is the electrical potential between the two ends of a circuit, and resistance within the circuit to the flow of current.

Operation cycle

A programmed series of commands that a device executes upon receiving a single start command. No additional commands are needed to complete the cycle.

Outlet box

A wall fixture containing a data jack or AC power receptacle.

Outside arming

A code or command that activates all security sensors to function while the home is unoccupied.

Overload

Current flow greater than a circuit can carry without danger of burning out.

Overloading

Placing a current demand on an electrical circuit above its capacity to carry safely.

Packet

A small segment into which data is divided and packaged with a header and trailer for transmission on a network.

PAL format

European analog TV standard equivalent to U.S. NTSC standard.

Panning motor

An accessory device for a surveillance video camera. The panning motor slowly swings the camera right and left, allowing it to cover more area than a stationary camera could.

Passive IR (PIR)

An IR sensor that doesn't emit any IR.

Passport

Older and slower type of power line technology for networking.

Password

A group of letters and numbers that must be entered into a security system in a home or into a computer system to gain access.

Patch panel

A device consisting of a row or block of jacks, used for connecting all components of a network.

PATHPING

An improved version of PING.

Peak use

The maximum load of electrical consumption in a home.

Peripheral

Any input or output device connected to a computer that sends or receives data from the processor. Examples of input peripherals are floppy drives and microphones. Examples of output peripherals are printers and control devices.

Phonograph

A machine that plays analog recordings from a plastic disc embossed with grooves bearing the sound wave impressions.

Piconet

A network of devices connected in an ad hoc fashion.

Picture frame lift

A motor-driven device that moves a picture frame upward to reveal what is behind it.

Pilot hole

A small hole drilled to locate a position or guide a larger drill bit.

Pilot light

A small flame that burns continuously in a furnace to ignite the furnace's main burner when it is turned on.

PING

A TCP/IP utility that enables a user at one computer to determine if that node can communicate with another computer connected to a network.

Pivot-down mechanism

A mechanism that is held in position on one side by a hinge and opens by swinging downward on that hinge to reveal its contents.

Pixel

A picture element in digital television; the unit of color and brightness that forms the picture in digital television.

Plain old telephone service (POTS)

The most common method of home Internet connection.

Plasma

Thin displays that typically use high definition standards. Composed of electrical circuits between two sheets of glass. Circuits create an electrical charge that creates the plasma and outputs light.

Platform lifts

Any motor-driven device intended to lift a piece of equipment or a display into a higher position for use or viewing.

Plug

A terminator on the end of a cable that mates with a jack to make a connection.

PPP (Point-to-Point Protocol) or SLIP (Serial Line Internet Protocol)

Most often is used to transmit TCP/IP packets from a computer connected to an ISP or intranet access point by telephone line.

Potential

The flow force of electric current, measured in volts.

Power conditioner

An electronic device that smoothes out the peaks and dips of household AC power. Also known as a line conditioner.

Power failure warning sensor

A device that detects the presence of voltage (electrical pressure) in a circuit and signals its absence to a monitor.

Power line network

Network technology that transmits data over a home's AC power lines at the same time high voltage power is running on the lines at a different frequency.

Powerline technology

Network data transmission method in which data signals are sent on AC wiring using a different frequency and voltage than the regular current flowing in the circuits.

PowerPacket

High speed power line technology for networking.

Preamplifier

A device that strengthens an original signal from an antenna or other source before it goes to an amplifier.

Pressure pads

A make switch that is closed when a set weight is placed on it. The sensor then signals its changed state.

Pressure sensor

A device that monitors gas or liquid pressure in a pipe or tank. If pressure drops too low (or, in a steam pipe, rises too high) the sensor signals the change.

Pressure valve

A type of valve that shuts off water flow automatically if pressure in the pipe drops below a set minimum, indicating that there is a leak or break in the pipe.

Private branch exchange (PBX)

A local switching point where phone lines within an organization can be connected to one another or to outside lines.

Program

A set of digital instructions that a computer executes in sequence to perform functions.

Programmable

Capable of storing instruction sets for later execution in sequence.

Progressive

Method of refreshing a video screen in which all lines are scanned in sequence.

Projector lift

A motor-driven device that lifts a projector from a concealed location and positions it for projecting an image on screen.

Protocol

A set of rules and standards that a network uses to communicate among its nodes.

Proximity reader

A device capable of reading an RFID keyfob or card held 4 to 24 inches from the device.

PTZ

Pan, tilt, zoom. Animated camera movement, either manual or automated, to enable the camera to cover a larger area by moving up/down, side to side, and zooming in or out.

Public switched telephone network (PSTN)

The commercial network of telephone lines and transmission facilities over which most telephone calls are made.

Pulling cable

The process of drawing a cable through an existing structure from one connector to another.

Pulse code modulation (PCM)

The method used to record compact discs using MP-2 compression. Not a magnetic process. Uses light diffraction to record data.

Punchdown block

The usual means of centrally terminating telephone lines and connecting them to the trunk lines.

PVC

Polyvinylchloride; a hard, strong plastic used to make pipe and many other products.

QAM

Quadrature Amplitude Modulation. The format by which digital cable is encoded and transmitted via cable.

QoS

Quality of Service is a measure of how to guarantee that packets in a VoIP system are not dropped or delayed due to network traffic.

Quicktime

An Internet and computer video file format that uses compression and is widely used by PC and Apple computers.

Raceway

An enclosed track in which to run cable; the track is attached to the surface of walls.

Radiant

A type of heating system that works by warming a home with hot water that flows to radiators in each room or in pipes beneath the floors. The radiators or floors then warm the interior air.

Radio frequency (RF)

Any electronic wave with a frequency in the radio band of the electromagnetic spectrum. Includes all radio and TV frequencies.

RadioRA

A proprietary wireless lighting control technology developed by Lutron and used for home lighting control.

Rain sensor

A device that detects the presence of rain water in a small holder and signals to the controller when a preset level is reached.

Rasters

The individual horizontal scan lines that make up an analog television picture.

Real-time antivirus scanner

Software that's designed to scan every file accessed on a computer so that it can catch viruses and worms before they can infect a computer.

RealVideo

A computer and Internet video compression algorithm.

Receptacle

A device into which AC-powered appliances can be plugged to obtain power.

Recessed

Concealed below (or above) a flat surface, usually with a covering that matches or complements the surface.

Record

A plastic disc with grooves bearing sound wave impressions that can be played on a phonograph.

Recorded emergency message

A message recorded on a security system call-in device; it plays after a device calls a preset telephone number and gets a connection. Some systems dial multiple numbers in succession and some can play multiple messages.

Redundant protection

In a security system, having two or more sensors or detectors monitoring one area or entrance. Provides additional security to high-risk areas.

Refresh rate

The number of times per second that the electron beam in a CRT repaints the entire screen.

Refrigerant fluid

A gas/liquid that circulates in an A/C system continuously extracting heat from the surrounding air as it changes from a liquid to a gas and back again.

Refrigeration

A method of cooling air that uses the heat absorption of expanding gas to extract heat from the surrounding air.

Regenerator

A digital data amplifier that reads weakened data signals and recreates them at full strength and without noise on the transmission line.

Relay

A remotely operated electric switch that is controlled by a small current, but that controls a large current flow.

Release and renew

If you need to update IP addressing information, you can remove the DHCP address that's been assigned to you and then manually send a request to the DHCP server for another IP address.

Remote access

Security system monitored by an outside commercial firm through a telephone or radio connection to the home control panel.

Remote control system

A combination of hardware and software that allows a person or a computer to direct the operation of a subsystem from a distance.

Repeater

A device in a LAN that receives and strengthens the data signal to offset its attenuation over distance.

Residential gateway

A device that connects a LAN with a WAN that is part of the Internet; the gateway controls the data coming into or going out of the LAN.

Resistance

The force inhibiting the flow of electricity in a circuit, measured in ohms.

Resolution

The number of pixels on a monitor that are individually addressable by software.

Response devices

Security devices that can perform an action when commanded to do so by the security panel. They may sound alarms, call for assistance, activate systems, or perform other tasks.

Retrofit

To add new wiring or other infrastructure to an existing building.

RJ-11 jack

The standard single line telephone connector wired with two wires.

RJ-14 jack

The standard two-line telephone connector wired with four wires.

RJ-45 crimping tool

A tool used to attach an RJ-45 plug as a terminator on the end of a cable.

RJ-45 jack

A terminator device on a cable into which a plug is mated to make a network connection.

RJ-45 punchdown tool

A tool used to attach an RJ-45 jack as a terminator on the end of a cable.

Rough in

To install the outlet boxes and cable runs for a network.

Routable

A protocol that allows data to be sent to interconnected networks on the Internet.

Router

A device that connects two or more networks and directs the data traffic passing between them.

SACD

Super Audio CD. A high-quality optical audio disc designed by Sony and Phillips.

Safety control valve

A specialized valve on the fuel line of a furnace or other appliance that must receive a continuous electric current from a thermocouple in order to stay open. If the current stops, the valve closes, shutting off the fuel flow.

Sampling

A technique for converting analog signals into digital form by taking quantified samples of the analog data.

Satellite link

An Internet connection to an ISP via a satellite through a receiver dish antenna.

Satellite transmission

Digital television signals beamed to receivers on the ground from a stationary satellite orbiting Earth in space.

Scan

Survey of a data set, space, or sensors to determine if particular data or a set of conditions is present.

Scan rate

The number of times per second that the electron beam in a CRT repaints the screen from top to bottom. Same as refresh rate in progressive screens, equal to twice the refresh rate in interlaced screens.

SDTV television

A television that receives and displays all ATSC digital formats, but not necessarily at full high resolution.

SDTV tuner

An RF receiver that receives ATSC terrestrial digital television signals and decodes all Table 3 video formats.

SECAM

A French-created European equivalent of NTSC analog standard.

SSL (Secure Sockets Layer)

A protocol that was developed by Netscape to provide security between application protocols.

SET (Secure Electronics Transactions)

A protocol designed to offer a secure medium for credit card transactions. It uses digital signatures to verify that both parties involved in the transaction are who they say they are.

Security breach

An event that occurs any time a sensor signals a change of status to a security panel.

Security panel

The control center of a security system to which all of the system's sensors and surveillance devices report their status. The panel may also direct responses, record data, and sound alarms.

Security zone

An area in a home or its yard that is monitored by a specific group of sensors in the security system. Zones are set up with defined monitoring devices so that the location and nature of any security breach can be quickly identified.

Sensor

Any device that detects or measures human activity or environmental conditions and sends data regarding its measurement to a processor.

Sensors

Devices that monitor an object (door, window, floor area) or condition in or around the home and signal the security panel if its status varies significantly from normal.

Serial

A transmission protocol in which bits of data are sent one at a time across the medium.

Server

A computer or device on a network that provides network services or manages network resources.

Service line

The cable that brings electric power into a home from the utility.

Service panel

The wall box containing a home's circuit breakers to which the service line is connected.

Service provider

A company that provides data transmission service or other utility services to consumers.

Shade controller

A device into which the end of a window shade's control rod fits, allowing the motor-driven controller to control the shade by remote commands.

Shaft

Any vertical open space (sometimes enclosed with walls or by a tube) that extends through a building or the earth for some distance. Shafts provide open space for elevators to move in, or for cables, wiring, and other equipment.

Shielding

Metal webbing around a data line that grounds noise and interference before it can reach the data line.

Shock

Electric current flowing through a person.

SIA

Security Industry Association is an international trade association for the security industry. There is also a monitoring format named SIA.

Signal to noise ratio (S/N ratio)

The difference in sound level between the recorded audio and the background noise on any type of audio recording.

Single pole switches

An AC basic switch that opens or closes a circuit to control power to a fixture.

SIP

IETF VoIP protocol that makes use of UDP and TCP over port 5060.

Skype

A proprietary peer-to-peer VoIP protocol and VoIP system.

Smoke detector

A device that signals the presence of smoke in the air around it. It does not react to heat or flame, but only to the presence of smoke particles.

Soft phones

Software programs that display phone features (hold button, caller ID, message waiting) on the computer screen and route the calls through a handset or an earphone and microphone wired to the computer.

Soil moisture sensor

A device that can measure the electrical conductivity of the ground in which it's buried. This measurement allows it to detect the amount of water in the soil.

Solenoid valve

An automatic valve operated by an electromagnet that can be energized or turned off to open or close the valve. It is the main control device in automated water systems.

Space heaters

A small heater, usually electric, but sometimes gas fired, designed to heat a small area or room. Manually controlled.

Spark igniter

An electrical device that ignites the fuel in an oil or gas furnace when it starts.

Speaker level

Sound levels determined by the power of the amplifier's output.

Spike

A large but very brief increase in voltage or current flow in a circuit.

Split duplex outlets

An AC electrical outlet in which one receptacle is always live and the other is controlled by a switch.

Splitters

Devices which allow two or more telephones or peripherals to be connected to a single wall jack.

Spread spectrum

Spread spectrum signals constantly change frequency, a process known as hopping, to reduce the power requirements for transmission.

Spring-loaded door closer

A device with a strong spring and a hydraulic damper that slowly closes an open door. The strong spring pulls the door shut firmly, and the damper prevents it from acting too quickly.

Stairway lift

A motorized lift with guide rails angled to fit on a stairway so that the lift can move at an angle up and down the stairs.

Standard definition television (SDTV)

The approved format for U.S. digital television with a 4:3 aspect ratio and a 525 by 720 pixel screen.

Star topology

One type of network topology in which nodes are arranged in a star pattern.

Stateful inspection

When a router also acts as a firewall, it can be called a screening router, which might use a technique called stateful inspection.

Static

Noise or interference on a telephone line that is typically heard as a background crackling sound.

Static IP address

A manually assigned IP address.

Stepdown transformer

A device that lowers AC voltage to the level required by the equipment.

Stereo

Two soundtracks recorded from the left and right side of a musical performance to give balance and depth to the recording.

Storage device

A computer peripheral that can record and retrieve digital data on magnetic or other media.

STP cable

Shielded twisted-pair cable used for LANs.

Straight through cables

Cable wiring that is connected to the same terminator pins at both ends of the cable.

Studs

The 2 × 4 or 2 × 6 wood uprights in the walls of homes.

Subnet

The part of the IP address that defines the network address; the other part of the IP address defines the computer address.

Subnet masks

Its function is to separate the IP address into the network address and the computer address so that routers and other network devices know where to send data packets.

Subsystem

A group of hardware components and software set up to perform a specific task or function within a larger, multiple-function HTI system.

Surface wiring

Wiring run along the outside of a wall, usually in a raceway, although it can be bare.

Surge

A brief increase in voltage or current flow in a circuit.

Surge suppressor

A device for blocking surges and spikes in a circuit.

Surveillance video camera

A small video camera used in a home security system to monitor a yard or part of the home's interior. The camera's output can be displayed or recorded or both.

Swipe slots

An input device for plastic magnetic-striped keys. The plastic key is passed (swiped) through the slot in the device, which reads the key code and grants access.

Switch

An electrical device that completes (turns on) or opens (turns off) a circuit; a device used in a LAN to direct data traffic among the nodes.

Switchboard

A device to which a number of telephone lines are connected and that can switch any line to connect to any other.

Switched duplex outlets

An AC electrical outlet controlled by a switch that turns current to it on or off.

Switcher

A multiple video input panel with a single output to a monitor and a switch that allows the monitor to display any video input selected.

Swivel mechanisms

A motorized platform that can turn a display or piece of equipment left or right. Some types can rotate continuously at a steady pace.

Synchronized

Operating or playing together at the same rate. Stereo sound tracks are synchronized as are the picture and sound of a video program.

T1 line

A high-capacity telephone trunk line capable of simultaneously handling up to 24 voice lines or 1.5 Mbps of data.

Telecommunications

The general name for all communication and data functions carried on telephone lines or radio signals, or performed by telephone hardware and software.

Television lift

A motor-driven device that can lift a television set out of concealment and position it for viewing.

TELNET

A TCP/IP utility that allows a user in one location to access a computer in a remote location as if the user were physically sitting in front of the remote machine.

Temperature sensor

A device that measures the ambient air temperature and signals it to a security system monitor that can compare it to programmed instructions and take appropriate action.

Terminator

A device on an Ethernet that ends the data flow in a bus topology.

Thermocouple

A device that transforms heat into an electrical current. Used in gas appliances to monitor the pilot light. If the light goes out, the thermocouple stops generating electricity, thereby signaling a problem.

Thermostat

A special type of temperature sensor that sends a signal when air temperature reaches a preset level.

Three way switches

A type of AC switch that is used in pairs to turn a circuit on or off from two locations.

Tilt mechanism

A mechanical device designed to change the angle of an object for better viewing or to make its use easier.

Token ring

A type of network in which data flows in a circular pattern and is controlled by a token.

TRACERT

A TCP/IP utility that shows the complete path that data packets are taking from the computer to reach any given destination.

Track

In automated equipment, a metal channel with sides that guide wheels set in the track along a set path.

Trailer

Data attached to the end of a data packet.

Transformer

An electrical device for stepping voltage in a circuit up or down with an inverse increase or decrease in amperage.

Translator

Another term for a decoder that converts encrypted data into a readable form for display by an output device.

Transmission

The movement of data from one location to another. The data can be digital or analog and the locations close together or distant.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The most common protocol used to connect networks.

Triad

A set of three dots in a color monitor that in combination can produce all colors.

Trip switch

An electric switch that turns a circuit on or off when activated by a moving object hitting it. Used as a stop switch for lifts or as a safety check to keep a lift car from moving too far up or down.

Trunk line

A telephone line from a PBX to the telephone company that can be used by any of the telephones connected to the PBX.

Truss

The triangular structures that support a roof.

Tuner

The device in a radio or television that sets the one station frequency to be received and excludes all others.

Twisted pair wires

A set of two wires twisted around one another in a specific manner to improve data transmission in a high-speed cable.

Uncompressed original video footage

Digital video recorded without use of any algorithm to reduce file size. Produces large files that contain all digital data in sequential format.

Unified messaging

A computer-based system for storing messages from multiple sources. Storage is located on a PC's hard drive and the messages include voice mail, fax, and e-mail.

Universal Serial Bus (USB)

A bidirectional, isochronous, dynamically attachable serial interface for adding devices on a single bus.

UPB

Universal Powerline Bus.

UPS

Uninterruptible power supply. A device that protects electronic equipment and computers from brownouts and blackouts.

Valve

A device for controlling the flow of fluids (gases or liquids) in a pipe. Can be manually or automatically controlled.

Valve box

An open-bottom box sunk to its lid in the ground where the zone valves, and sometimes the controller of a sprinkler system, are located.

Ventilation

The process of exchanging air in a confined room or space. Ventilation exhausts the old air out of a room and brings new air in.

Vents

An opening in a wall or floor through which air flows from a connected duct into a room.

Video

A digital display of pictures such as television programs or computer screens.

Video conferencing

A technology for sending full-motion picture images with a voice telephone call so that callers can both hear and see one another.

Video distribution system

A wired system for distributing video programs from multiple sources to multiple viewing sites in the home.

Video Home Standard (VHS)

The U.S. standard analog video recording format used in video cassettes.

Video image

Any image, analog or digital, displayed on a CRT or other type of screen.

Video processor

Scales images for display on your TV. Converts from film to TV, between 4:3 and 16:9, and handles picture-in-picture windows.

Video server

A computer set up as a storage location for video programming on a network, from which the video footage can be requested by other network nodes.

Virus

A self-propagating program that is sent to a computer, remains resident in its storage, and can interfere with or disable its operation.

Voice messaging

A digital system that allows telephone callers to record messages that the system stores, retrieves, and plays on demand.

Voice over Internet Protocol (VoIP)

A system whereby analog phone calls are digitized and sent in packets over the Internet. At the destination, the digital data is decoded to analog form and delivered to the receiver.

VoIP DECT

VoIP digital enhanced cordless telecommunications is a radio access technology in which phones contain a WiFi transceiver rather than an Ethernet jack.

Voltage

The force of electricity caused by a difference in charge, or electrical potential at two locations.

Volts

The unit used to measure electric potential or flow pressure.

VSF

Vestigial side band. The RF modulation format used by digital TV to transmit digital bits to the home consumer.

Wall mounted controllers

In video and audio systems, a device for controlling distributed programming in a room or for the whole system.

War chalking

The process of marking buildings, curbs, and other landmarks indicating the presence of an available access point and its connection details by utilizing a set of symbols and shorthand.

Wardriving

Driving around in a car with a laptop using a wireless network card and identifying networks that are open for connection.

Water pressure

The force that impels water through a pipe. Water pressure is produced by gravity (the weight of water pushing down from higher elevation to a lower one) or by artificially pressurizing a sealed water system, usually with compressed air.

Water sensor

A device that senses the presence of water and signals it to a security monitor or panel.

Water service line

The pipe that supplies water to a residence from a public utility. It enters the home and connects to the interior plumbing and exterior water system.

Watts

The unit of electric power, often calculated for a circuit by multiplying the number of volts by the number of amps.

WAVE file

A compression algorithm for sound files.

WECA

Wireless Ethernet Compatibility Alliance. The former name of the WiFi Alliance.

WEP

Wired Equivalent Protocol. A protocol built on the 802.11 standards that governs how data can be encrypted while in transit on the wireless network.

Wiegand protocol

The protocol used by most access control card readers. The standard version is the 26-bit format with 24 bits of encrypted data.

WiFi (Wireless Fidelity)

IEEE 802.11b wireless standard with an 11-Mbps transmission rate. It is currently the most popular wireless standard.

WiFi5

IEEE 802.11a was designated by its promoters as WiFi5, a very high speed wireless technology.

Wind sensor

A device that can be set to signal a controller whenever the average wind speed rises to a preset level (adjustable from 12 to 35 miles per hour). Used to shut off sprinkler systems in high wind conditions.

Windows Media Audio (WMA)

An MPEG-4 audio compressed file.

WINPCFG

Windows 9x version of IPCONFIG, a utility for displaying a computer's adapter address, IP address, subnet mask, and default gateway and renewing or releasing its DHCP.

Wireless audio transmitter

A wireless transmitter that sends analog or digital audio signals to a computer.

Wireless hub

A device to which nodes in a wireless LAN can connect using radio waves.

Wireless NIC

A device in a wireless node that connects it to a hub using radio waves.

Wireless technology

Any of several methods of communicating digital data by means of radio waves without the need for any wires connecting the sender and receiver.

World Wide Web (WWW)

The global system of interconnected networks over which users can share data through the use of common protocols.

WPA

WiFi Protected Access. A wireless communication protocol that is replacing WEP. It uses a shared key for security.

X10

A wired technology that transmits data on existing high voltage AC power lines in the home, and thus requires no new wires for installation.

Z-Wave

A wireless home control protocol that can control up to 192 devices.

ZigBee

A wireless control protocol intended for use in applications with low data rates and low power consumption.

Zone

The area around a wireless hub that its transmission reaches and from which it can receive data from wireless nodes; in sprinkler systems, multiple sprinkler heads in an area that are controlled by one valve; in lighting systems, a group of lights controlled together to provide a specific scene or accomplish a specific task, such as security lighting.

Index

A

A/V components
 Configuring, 3-38
 Access control, 1-7
 Access point (AP), 2-76
 Acoustics, 3-4
 Active Directory, 2-5
 ActiveX controls, 2-72
 Advanced Television Systems Committee (ATSC)
 standard, 3-20
 Analog telephone system, 4-2, 4-13
 AppleTalk, 2-19
 Associated Standard Code for Information Interchange
 (ASCII), 6-12
 Audio
 Reception for, 1-5
 Automatic Private IP Addressing (APIPA), 2-21
 Automation, 1-7

B

Biometric identification systems, 5-23
 Bluetooth, 6-9
 Butt set, 7-26

C

Cable modems, 2-38
 Cable service, 1-6
 Cable television, 3-29
 Cable testing devices, 7-5, 7-6
 Cable types, 3-37
 Camera types, 5-29
 Cameras
 Installing, 5-42
 Carbon monoxide detectors, 5-6
 Card readers, 5-22
 Cathode ray tube (CRT), 3-15
 CEA-ComPTIA DHTI+, 1-3
 Client for Microsoft Networks, 2-28
 Communication links, 1-16
 Content sources, 3-27, 3-28, 3-29, 3-30
 Continuity, measuring, 7-4
 Control devices, 1-18
 Control systems
 PC-based, 6-3
 Controllers
 Programming, 6-21
 Cookies, 2-68
 Crossover, 3-7, 3-8

Crosstalk, 4-11
 Current
 Measuring, 7-4

D

Default gateway, 2-24
 Delays, 5-27
 Digital Addressable Lighting Interface (DALI), 6-34
 Digital Home Technology Integration (DHTI), 1-2
 Digital light processor (DLP), 3-18
 Digital rights management (DRM), 3-34
 Digital Subscriber Line (DSL), 4-14
 Digital telephone system, 4-13
 Digital Theater System (DTS), 3-9
 Digital TV, 3-20
 Directory service, 2-26
 Distribution
 Digital, 3-41
 RF, 3-41
 Distribution panel, 1-19
 Documentation, 7-9
 Documenting the installation, 1-26, 1-27
 Dolby Digital (DD), 3-10
 Domain controllers, 2-3, 2-6
 Domain Name Service (DNS), 2-6
 DSL, 2-39
 DVD-Audio (DVD-A), 3-11
 Dynamic Host Configuration Protocol (DHCP), 2-6

E

Electrical connections
 Daisy chain, 6-31
 Home run, 6-31
 Embedded control systems, 6-2
 Environmental sensors, 5-6
 Installing, 5-44
 Extended Surround format, 3-10

F

Fax machines, 4-9
 File and Printer Sharing for Microsoft Networks, 2-28
 Filters, 7-17
 Fire alarms, 5-5
 Firewalls, 2-52
 Hardware, 2-53
 Port and packet filters, 2-54
 Software, 2-54
 FTP, 2-36

G

Gas leak detectors, 5-6
Glass-break detector, 5-3

H

HTI
 Basic components of, 1-14
 Benefits of, 1-11
 Credentials for, 1-23
 Definition of, 1-2
 Functions of, 1-5
HTML, 2-35
HTTP, 2-36
HVAC
 Communication layer, 6-17
 Control layer, 6-16
 Master/slave relationship, 6-18
 Ventilation, 6-19

I

IEEE 802.11 standard, 2-76
IMAP, 2-35
Impedance, 3-6
InfraRed (IR) detection, 5-2
Infrared transmissions, 6-8
Infrastructure
 Types of, 5-14
Inoculation, 2-61
Institute of Electronic and Electric Engineers (IEEE), 2-77
Interference, 7-15
Internet
 Connections, 2-44
 Technologies, 2-34
 Web browsers, 2-70
Internet connectivity
 Cable, 1-5
 DSL, 1-5
 Telephone lines, 1-5
Internet service providers (ISPs), 1-25
Internet zone, 2-71
Intranets, 2-70
IP addresses, 2-21
 Static, 2-21
IPX/SPX, 2-19
IR protocol, 6-8
ISDN, 2-39

J

Jitter, 4-22

K

Key systems, 4-28
Keyfobs, 5-9, 6-4
Keypads, 5-8, 5-21, 6-4

L

Labeling wires, 1-26
Latency, 4-22
Lighting control applications, 6-26
Lighting systems
 Planning, 6-30
 Requirements, 6-29
 Zones, 6-30
Line seizure devices, 5-15
Line-level audio, 3-5
Linux, 2-5, 2-8
Linux operating system, 6-2
Liquid crystal display (LCD), 3-17
Liquid Crystal on Silicon (LCoS), 3-18
Local intranet zone, 2-71
Lux rating, 5-31

M

Macintosh, 2-9
Matrixed channels, 3-9
Media access control (MAC) addresses, 2-12
Memory cards, 3-32
Microsoft Knowledge Base, 7-10
Modem communications, 4-9
Monitoring devices, 1-18
Motion sensors, 5-2
Multi-channel surround sound, 3-8
Multimeters, 7-2
Multi-room Audio Video (MRAV) standard, 3-25

N

National Television Standards Committee (NTSC)
 standard, 3-20
Native Wireless Fidelity, 2-86
NetBEUI, 2-19
Network interface cards (NICs), 2-7
Network operating systems (NOSs), 2-4
Networking
 TCP/IP configuration, 2-21
 Windows workgroups and domains, 2-26
Networking devices
 Network interface cards (NICs), 2-10
Networks
 Client/server, 2-3
 Firewalls, 2-6
 Name resolution, 2-6
 Operating systems, 2-4, G-13
 Peer-to-peer, 2-3
 Protocols, 2-19
 Services, 2-6
Nodes, 2-19
Notification methods, 5-15

O

Ohm's law, 3-6

P

Packet loss, 4-22
Passive IR (PIR) sensors, 5-2
PC-based control systems, 6-3
Peer-to-peer networks, 2-3
Piconets, 6-9
Plain Old Telephone Service (POTS), 4-2
Plasma, 3-17
Pop-up ads, 2-64
Post Office Protocol, 2-35
PowerLine Carrier, 6-35
PPPoE, 2-38
Pressure sensors, 5-7
Private branch exchange (PBX) telephone systems, 4-24, 4-25
Processors, 1-15
Proprietary protocols, 6-13
Proximity readers, 5-24
Public Safety Answering Point (PSAP), 4-16

Q

Quality of Service (QoS), 4-22

R

Radio communications, 6-9
Radio interference, 4-11
Recording devices, 1-19
Release and renew, 2-22
Remote controls, 6-3
Resistance
 Measuring, 7-3
Resource sharing, 2-28, 2-31
 Printers, 2-32
Restricted sites zone, 2-72
Ringer Equivalency Number (REN), 4-11

S

Satellite, 2-39
Satellite broadcast, 3-28
Satellite service, 1-6
Secure Electronics Transactions (SET), 2-60
Secure Sockets Layer (SSL), 2-58
Security, 1-7
 Antivirus software, 2-60
 Electronic transaction protocols, 2-58
 Intrusion detection, 2-58
Security systems
 Installing, 5-38
 Wireless, 5-17
Security zones, 2-71
Sensors, 1-17
 Types of, 1-18
Serial transmission, 6-10
Shielding, 7-17
S-HTTP, 2-36
SIA monitoring format, 5-11

Simple File Sharing, 2-29
Skype, 4-19
Smoke detectors, 5-5
SMTP, 2-35
Snow detectors, 5-6
Soft phones, 4-15
Sound cancellation, 3-7
Spam, 2-64
Speaker placement, 3-4
Speakers
 Specifications, 3-13
 Types of, 3-11
Spyware, 2-66
SSL, 2-36
standard 802.1x, 2-75
Subnet masks, 2-22
Subnets, 2-21
Super Audio CD (SACD), 3-10
Surge protectors, 6-41
Switches, 6-28
System recovery, 7-30
System testing, 5-46

T

TCP/IP, 2-19
Technology
 Benefits of, 1-11, 1-12
Telecommunications, 1-6
Telephone installation, 4-5
Telnet, 2-36
Temperature sensors, 5-4
Thermostats, 6-21
Touch screens, 6-5
Troubleshooting, 7-7
 ASID model, 7-8
 Networks, 7-19
Trusted sites zone, 2-71

U

Unified messaging, 4-30
Uninterruptible power supply (UPS), 5-28
Universal Naming Convention (UNC), 2-31
Universal Powerline Bus (UPB), 6-36
UNIX, 2-5
User interfaces, 6-3
Utilities
 Managing, 1-8

V

Video
 Reception for, 1-5
Video processing, 3-22
Virus definitions, 2-61
Voice messaging, 4-30
Voice over IP (VoIP) systems, 4-14
Voice over IP systems, 4-16
Voltage

Measuring, 7-3

W

War chalking, 2-78
Wardriving, 2-78
Water sensors, 5-5
Weather sensors, 2-70
Web browsers, 2-70
Web tablets, 6-5
Wiegand protocol, 5-25
Wi-Fi, 2-86
Wi-Fi Protected Access (WPA), 2-83
Windows Internet Naming Service (WINS), 2-6
Wire mapping, 1-26
Wireless, 2-40
Wireless access points
 802.1x, 2-83
 Configuration, 2-82
 Enabling, 2-82
 Factory settings, 2-82
 MAC filters, 2-82
 Wi-Fi Protected, 2-83
Wireless Auto Configuration, 2-85
Wireless clients, 2-85

Windows 2000, 2-86

Windows CE, 2-86

Windows XP, 2-85

Wireless Ethernet Compatibility Alliance (WECA), 2-77

Wireless security systems, 5-17

Wireless Zero Configuration, 2-85

WLAN

 Security, 2-77

WLAN technology

 Wireless standards, 2-75

X

X10 power-line systems

 Components, 5-18

Z

ZigBee, 6-35

ZigBee protocol, 6-12

Zones, 2-19

Z-Wave, 6-34

Z-Wave standard, 6-12