Course Booklet

CCNA Discovery

Working at a Small-to-Medium Business or ISP

Version 4.1

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

CCNA Discovery Course Booklet Working at a Small-to-Medium Business or ISP, Version 4.1

Cisco Networking Academy

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing October 2009

Library of Congress Cataloging-in-Publication Data is on file.

ISBN-13: 978-1-58713-253-7

ISBN-10: 1-58713-253-2

Warning and Disclaimer

This book is designed to provide information about working for a small-to-medium business or ISP. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Erik Ullanderson

Cisco Press Program Manager
Anand Sundaram

Executive Editor
Mary Beth Ray

Managing Editor
Patrick Kanouse

Project Editor
Bethany Wall

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Composition
Mark Shirar

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.cisco.com/edu.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Course Introduction

Welcome

Welcome to the CCNA Discovery course, Working at a Small-to-Medium Business or ISP. The goal of this course is to assist you in developing the skills necessary to provide customer support to users of small-to-medium-sized networks and across a range of applications. The course provides an introduction to routing and remote access, addressing and network services. It will also familiarize you with servers providing email services, web space, and Authenticated Access. This course prepares you with the skills required for entry-level Help Desk Technician and entry-level Network Technician jobs.

More than just information

This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and grade book
- Packet Tracer 4.1 simulation tool
- Additional software for classroom activities

A global community

When you participate in the Networking Academy, you are joining a global community linked by common goals and technologies. Schools, colleges, universities and other entities in over 160 countries participate in the program. You can see an interactive network map of the global Networking Academy community at http://www.academynetspace.com.

The material in this course encompasses a broad range of technologies that facilitate how people work, live, play, and learn by communicating with voice, video, and other data. Networking and the Internet affect people differently in different parts of the world. Although we have worked with instructors from around the world to create these materials, it is important that you work with your instructor and fellow students to make the material in this course applicable to your local situation.

Keep in Touch

These online instructional materials, as well as the rest of the course tools, are part of the larger Networking Academy. The portal for the program is located at http://cisco.netacad.net. There you will obtain access to the other tools in the program such as the assessment server and student grade book), as well as informational updates and other relevant links.

Mind Wide Open®

An important goal in education is to enrich you, the student, by expanding what you know and can do. It is important to realize, however, that the instructional materials and the instructor can only facilitate the process. You must make the commitment yourself to learn new skills. Below are a few suggestions to help you learn and grow.

1. Take notes. Professionals in the networking field often keep Engineering Journals in which they write down the things they observe and learn. Taking notes is an important way to help your understanding grow over time.
2. Think about it. The course provides information both to change what you know and what you can do. As you go through the course, ask yourself what makes sense and what doesn't. Stop and ask questions when you are confused. Try to find out more about topics that interest you. If you are not sure why something is being taught, consider asking your instructor or a friend. Think about how the different parts of the course fit together.
3. Practice. Learning new skills requires practice. We believe this is so important to e-learning that we have a special name for it. We call it e-doing. It is very important that you complete the activities in the online instructional materials and that you also complete the hands-on labs and Packet Tracer® activities.
4. Practice again. Have you ever thought that you knew how to do something and then, when it was time to show it on a test or at work, you discovered that you really hadn't mastered it? Just like learning any new skill like a sport, game, or language, learning a professional skill requires patience and repeated practice before you can say you have truly learned it. The online instructional materials in this course provide opportunities for repeated practice for many skills. Take full advantage of them. You can also work with your instructor to extend Packet Tracer, and other tools, for additional practice as needed.
5. Teach it. Teaching a friend or colleague is often a good way to reinforce your own learning. To teach well, you will have to work through details that you may have overlooked on your first reading. Conversations about the course material with fellow students, colleagues, and the instructor can help solidify your understanding of networking concepts.
6. Make changes as you go. The course is designed to provide feedback through interactive activities and quizzes, the online assessment system, and through interactions with your instructor. You can use this feedback to better understand where your strengths and weaknesses are. If there is an area that you are having trouble with, focus on studying or practicing more in that area. Seek additional feedback from your instructor and other students.

Explore the world of networking

This version of the course includes a special tool called Packet Tracer 4.1®. Packet Tracer is a networking learning tool that supports a wide range of physical and logical simulations. It also provides visualization tools to help you to understand the internal workings of a network.

The Packet Tracer activities included in the course consist of network simulations, games, activities, and challenges that provide a broad range of learning experiences.

Create your own worlds

You can also use Packet Tracer to create your own experiments and networking scenarios. We hope that, over time, you consider using Packet Tracer – not only for experiencing the activities included in the course, but also to become an author, explorer, and experimenter.

The online course materials have embedded Packet Tracer activities that will launch on computers running Windows® operating systems, if Packet Tracer is installed. This integration may also work on other operating systems using Windows emulation.

CHAPTER 3

Planning a Network Upgrade

Introduction

3.1 Documenting the Existing Network

Refer to **Figure** in online course

3.1.1 Site Survey

Refer to **Figure** in online course

When a small company grows rapidly, the original network that supports the company often cannot keep pace with the expansion. Employees at the company may not realize how important it is to plan for network upgrades. The business may just add network hardware devices of varying quality from different manufacturers and different network connection technologies to connect new users. The quality of the current network may become degraded as each new user is added, until it can no longer support the level of network traffic that the users generate.

When the network starts to fail, most small businesses look for help to redesign the network to meet the new demands. An ISP or managed service provider may be called in to provide advice, and to install and maintain the network upgrade.

Before a network upgrade can be properly designed, an on-site technician is dispatched to perform a site survey to document the existing network structure. It is also necessary to investigate and document the physical layout of the premises to determine where new equipment can be installed.

Refer to **Figure** in online course

A site survey provides the network designer important information and creates a proper starting point for the project. It shows what is already on site, and gives a good indication as to what is needed.

Important pieces of information that can be gathered during a site survey include:

- Number of users and types of equipment
- Projected growth
- Current Internet connectivity
- Application requirements
- Existing network infrastructure and physical layout
- New services required
- Security and privacy considerations
- Reliability and uptime expectations
- Budget constraints

It is a good idea to obtain a floor plan, if possible. If a floor plan is not available, the technician can draw a diagram indicating the size and location of all rooms. An inventory of existing network hardware and software is also useful to provide a baseline of requirements for the upgrade.

A sales representative may also accompany the technician to the site to interview the customer. The sales representative may ask a series of questions to gather information about the network upgrade needs of the business.

Refer to **Figure** in online course

The technician should be prepared for anything when doing the site survey. Networks do not always meet local codes of practice in terms of electrical, building, or safety regulations, nor adhere to any standards.

Sometimes networks grow haphazardly over time and end up being a mixture of technologies and protocols. The technician should be careful not to offend the customer by expressing an opinion about the quality of the existing installed network.

When visiting the customer premises, the technician should do a thorough overview of the network and computer setup. There may be some obvious issues such as unlabeled cables, poor physical security for network devices, lack of emergency power, or lack of an uninterruptible power supply (UPS) for critical devices. These conditions are noted in the site survey report, in addition to the other requirements gathered from the survey and the customer interview.

When the site survey is completed, it is important that the technician review the results with the customer to ensure that nothing is missed and that there are no errors. If everything is accurate, the site survey provides an excellent basis for the new network design.

3.1.2 Physical and Logical Topologies

Refer to **Figure** in online course

Both the physical and logical topology of the network must be documented. A physical topology is the actual physical location of cables, computers, and other peripherals. A logical topology documents the path that data takes through the network and where network functions, like routing, occur. A technician gathers this information during the site survey to create the physical and logical topology map.

In a wired network, the ***physical topology*** map consists of the wiring closet and the wiring to the individual end-user stations. In a wireless network, the physical topology consists of the wiring closet and an access point. Because there are no wires, the physical topology contains the wireless signal coverage area.

The ***logical topology*** is generally the same for a wired and wireless network. It includes the naming and Layer 3 addressing of end stations, router gateways, and other network devices, regardless of the physical location. It indicates the location of routing, network address translation, and firewall filtering.

Refer to **Figure** in online course

To develop a logical topology requires understanding the relationship between the devices and the network, regardless of the physical cabling layout. There are several topological arrangements possible. Examples include star, extended star, partial mesh, and full mesh topologies.

Star Topologies

With a star topology, each device is connected via a single connection to a central point. The central point is typically a switch or a wireless access point. The advantage of a star topology is that if a single connecting device fails, only that device is affected. However, if the central device, such as the switch, fails, then all connecting devices lose connectivity.

An extended star is created when the central device in one star is connected to a central device of another star, such as when multiple switches are interconnected, or daisy-chained together.

Mesh Topologies

Most Core Layers in a network are wired in either a full mesh or a partial mesh topology. In a full mesh topology, every device has a connection to every other device. While full mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly.

For larger installations, a modified partial mesh topology is used. In a partial mesh topology, each device is connected to at least two other devices. This arrangement creates sufficient redundancy, without the complexity of a full mesh.

Implementing redundant links through partial or full mesh topologies ensures that network devices can find alternate paths to send data in the event of a failure.

3.1.3 Network Requirements Documentation

Refer to **Figure** in online course

Along with creating the topology maps for the existing network, it is necessary to obtain additional information about the hosts and networking devices that are currently installed. This information is recorded on a brief inventory sheet. The technician also documents any growth that the company anticipates in the near future.

This information helps the network designer determine what new equipment is required, and the best way to structure the network to support the anticipated growth.

The inventory sheet of the installed devices includes:

- Device name
- Date of purchase
- Warranty information
- Location
- Brand and model
- Operating system
- Logical addressing information
- Gateway
- Method of connectivity
- Virus Checker
- Security information

Refer to **Packet Tracer Activity** for this chapter

Packet Tracer Activity

Create a logical and physical network diagram.

View printable instructions.

3.2 Planning

3.2.1 Network Upgrade Planning Phases

Refer to **Figure** in online course

A network upgrade requires extensive planning. Just like any project, a need is identified and then a plan outlines the process from beginning to end. A good project plan helps identify any

strengths, weaknesses, opportunities, or threats (***SWOT***). The plan clearly defines the tasks, and the order in which the tasks are to be completed.

Examples of good planning:

- Sports teams follow game plans
- Builders follow blueprints
- Ceremonies or meetings follow agendas

A network that is a patchwork of devices strung together, using a mixture of technologies and protocols, is usually an indicator of poor initial planning. These types of networks are susceptible to downtime, and are difficult to maintain and troubleshoot.

Refer to **Figure** in online course

Planning a network upgrade begins after the site survey and the resulting report are completed. There are five distinct phases.

Phase 1: Requirements Gathering

After all of the information has been gathered from the customer and the site visit, it is analyzed to determine the network requirements. This analysis is done by the design team at the ISP, which creates an Analysis Report.

Phase 2: Selection and Design

Devices and cabling are selected based on the requirements outlined in the ***Analysis Report***. Multiple design options are created and regularly shared with other members on the project. This phase allows team members to view the network from a documentation perspective and evaluate trade-offs in performance and cost. It is during this step that any weaknesses of the design can be identified and addressed.

Also during this phase, prototypes are created and tested. A ***prototype*** is a good indicator of how the new network will operate.

When the design is approved by the customer, implementation of the new network can begin.

Phase 3: Implementation

If the first two steps are done correctly, the implementation phase is more likely to be performed without incident. If there are tasks that have been overlooked in the earlier phases, they must be corrected during implementation. Creating an implementation schedule that allows time for unexpected events, keeps disruption for the customer to a minimum. Staying in constant communication with the customer during the installation is critical to the success of the project.

Refer to **Figure** in online course

Phase 4: Operation

The network is brought into service in what is called a ***production environment***. Prior to this step, the network is considered to be in a testing or implementation phase.

Phase 5: Review and Evaluation

After the network is in operation, the design and implementation must be reviewed and evaluated. For this process, the following steps are recommended:

Step 1: Compare the user experience with the goals in the documentation, and evaluate if the design is right for the job.

Step 2: Compare the projected designs and costs with the actual deployment. This evaluation ensures that future projects will benefit from the lessons learned on this project.

Step 3: Monitor the operation and record changes. It is important that the system is always fully documented and accountable.

Careful planning at each phase ensures that the project goes smoothly and that the installation is successful. On-site technicians are often included in the planning, because they participate in all phases of the upgrade.

Refer to **Interactive Graphic** in online course.

Activity

Determine if an action is part of the Requirements Gathering, Selection and Design, Implementation, Operation, or Review and Evaluation phase.

Based on the statement, select the appropriate phase.

3.2.2 Physical Environment

Refer to **Figure** in online course

One of the first things that the network designer does to select the equipment and design of the new network is to examine the existing network facilities and cabling. The facilities include the physical environment, the telecommunication room, and the existing network wiring. A ***telecommunications room***, or wiring closet, in a small, single-floor network is usually referred to as the Main Distribution Facility (***MDF***).

The MDF typically contains many of the network devices, including switches or hubs, routers, and access points. It is where all of the network cable concentrates to a single point. Many times, the MDF also contains the Point of Presence (POP) of the ISP, where the network makes the connection to the Internet through a telecommunications service provider.

If additional wiring closets are required, they are referred to as Intermediate Distribution Facilities (IDFs). IDFs are typically smaller than the MDF, and connect to the MDF.

Many small businesses do not have a telecommunications room or closet. Network equipment may be located on a desk or other furniture, and wires could be just lying on the floor. Network equipment must always be secure. As a network grows, a telecommunications room is critical to the security and reliability of the network.

3.2.3 Cabling Considerations

Refer to **Figure** in online course

When the existing cabling is not up to specification for the new equipment, new cabling must be planned for and installed. The condition of the existing cabling can quickly be determined by the physical inspection of the network during the site visit. When planning the installation of network cabling, there are four physical areas to consider:

- User work areas
- Telecommunications room
- Backbone area
- Distribution area

There are many different types of cable found in the networking environment, and some are more common than others:

- ***Shielded twisted pair (STP) -*** Usually Category 5, 5e, or 6 cable that has a foil shielding to protect from outside electromagnetic interference (EMI). In an Ethernet environment, the distance limitation is approximately 328 feet (100 meters).

- ***Unshielded twisted pair (UTP) -*** Usually Category 5, 5e, or 6 cable that does not provide extra shielding from EMI, but it is inexpensive. Cable runs should avoid electrically noisy areas. In an Ethernet environment, the distance limitation is approximately 328 feet (100 meters).
- ***Fiber-optic cable -*** A medium that is not susceptible to EMI, and can transmit data faster and farther than copper. Depending on the type of fiber optics, distance limitations can be several miles (kilometers). Fiber-optic can be used for backbone cabling and high-speed connections.

In addition to these three commonly-used cabling types, coaxial is also used in networking. Coaxial is not typically used in LANs, but it is widely used in cable modem provider networks. Coaxial has a solid copper core with several protective layers including polyvinyl chloride (PVC), braided wire shielding, and a plastic covering. Distance is several miles (kilometers). Limitations depend on the purpose of the connection.

There are several organizations in the world that provide LAN cabling specifications.

Refer to **Figure** in online course

The Telecommunications Industry Association (TIA) and the Electronic Industries Alliance (EIA) worked together to provide the TIA/EIA cable specifications for LANs. Two of the most common TIA/EIA cable specifications include the 568-A and 568-B standards. Both of these standards typically use the same Cat 5 or Cat 6 cable, but with a different termination color code.

There are three different types of twisted pair cables that are used in networks:

- ***Straight-through -*** Connects dissimilar devices, such as a switch and a computer, or a switch and a router.
- ***Crossover -*** Connects similar devices, such as two switches or two computers.
- **`Console`** (or Rollover) - Connects a computer to the console port of a router or switch to do initial configuration.

Another cable type that is common in networks is a ***serial cable***. A serial cable is typically used to connect the router to an Internet connection. This Internet connection may be to the phone company, the cable company, or a private ISP.

3.2.4 Structured Cable

Refer to **Figure** in online course

When designing a structured cable project, the first step is to obtain an accurate floor plan. The floor plan allows the technician to identify possible wiring closet locations, cable runs, and which electrical areas to avoid.

After the technician has identified and confirmed the locations of network devices, it is time to draw the network on the floor plan. Some of the more important items to document include the following:

- ***Patch cable -*** Short cable from the computer to the wall plate in the user work area
- ***Horizontal cable -*** Cable from the wall plate to the IDF in the distribution area
- ***Vertical cable -*** Cable from the IDF to the MDF in the backbone area of the business
- ***Backbone cable -*** Network part that handles the major traffic
- ***Location of wiring closet -*** Area to concentrate the end-user cables to the hub or switch
- ***Cable management system -*** Trays and straps used to guide and protect cable runs
- ***Cable labeling system -*** Labeling system or scheme to identify cables

- ***Electrical considerations -*** Outlets and other items to support the electrical requirements of the network equipment

Refer to
Lab Activity
for this chapter

Lab Activity

Evaluate a floor plan and propose upgrades to accommodate extra floor space.

3.3 Purchasing and Maintaining Equipment

3.3.1 Purchasing Equipment

Refer to
Figure
in online course

As the ISP team plans the network upgrade, issues related to purchasing new equipment and the maintenance of new and existing equipment must be addressed. There are generally two options for obtaining new equipment:

- ***Managed service -*** The equipment is obtained from the ISP through a lease or some other agreement, and the ISP is responsible for updating and maintaining the equipment.
- ***In-house -*** The customer purchases the equipment, and the customer is responsible for the updates, warranties, and maintenance of the equipment.

When acquiring equipment, cost is always a major factor. A good cost analysis of the various options provides a sound basis for the final decision.

If a managed service is chosen, there are lease costs and possibly other service costs as outlined in the Service Level Agreement (SLA).

If the equipment is purchased outright, the customer should be aware of the price of the equipment, warranty coverage, compatibility with existing equipment, and update and maintenance issues. All of these must be analyzed to determine the cost-effectiveness of the purchase.

3.3.2 Selecting Network Devices

Refer to
Figure
in online course

After analyzing requirements, the design staff recommends the appropriate network devices to connect and support the new network functionality.

Modern networks use a variety of devices for connectivity. Each device has certain capabilities to control the flow of data across a network. A general rule is that the higher the device is in the OSI model, the more intelligent it is. What this means is that a higher level device can better analyze the data traffic and forward it based on information not available at lower layers. As an example, a Layer 1 hub can forward data only out of all ports, while a Layer 2 switch can filter the data and send it only out of the port that is connected to the destination based on the MAC address.

As switches and routers evolve, the distinction between them may seem blurred. One simple distinction remains: LAN switches provide connectivity within the local-area networks of the organization, while routers interconnect local networks and are needed in a wide-area network environment.

In addition to switches and routers, there are other connectivity options available for LANs. Wireless access points allow computers and other devices, such as handheld IP phones, to wirelessly connect to the network or share broadband connectivity. Firewalls guard against network threats and provide security and network control and containment.

Integrated Service Routers (ISRs) are network devices that combine the functionality of switches, routers, access points, and firewalls into the same device.

3.3.3 Selecting LAN Devices

Refer to **Figure** in online course

Although both a hub and a switch can provide connectivity at the Access Layer of a network, switches should be chosen for connecting devices to a LAN. Switches are more expensive than hubs, but the enhanced performance makes switches more cost-effective. A hub is generally chosen as a networking device only within a very small LAN, a LAN that requires little ***throughput*** requirements, or when finances are limited.

When selecting a switch for a particular LAN, there are a number of factors to consider. These factors include, but are not limited to:

- Speed and the types of ports and interfaces involved
- Expandability
- Manageability
- Cost

Speed and Types of Ports and Interfaces

Choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without replacing the central devices.

When selecting a switch, choosing the appropriate number and type of ports is critical.

Network designers should consider carefully how many twisted pair (TP) and fiber-optic ports are needed. It is also important to estimate how many more ports will be required to support network expansion.

Refer to **Figure** in online course

Expandability

Networking devices come in both fixed and modular physical configurations. Fixed configurations have a specific type and number of ports or interfaces. Modular devices have expansion slots that provide the flexibility to add new modules as requirements evolve. Most modular devices come with a minimum number of fixed ports and expansion slots.

A typical use of an expansion slot is to add fiber-optic modules to a device originally configured with a number of fixed TP ports. Modular switches can be a cost-effective approach to scaling LANs.

Manageability

A basic, inexpensive switch is not configurable. A managed switch that uses a Cisco IOS feature set allows control over individual ports or over the switch as a whole. Controls include the ability to change the settings for a device, add port security, and monitor performance.

For example, with a managed switch, ports can be turned on or off. In addition, administrators can control which computers or devices are allowed to connect to a port.

Refer to **Figure** in online course

Cost

The cost of a switch is determined by its capacity and features. The switch capacity includes the number and types of ports available and the overall throughput. Other factors that affect the cost are network management capabilities, embedded security technologies, and advanced switching technologies.

Using a simple cost-per-port calculation, it may initially appear that the best option is to deploy one large switch at a central location. However, this apparent cost savings may be offset by the expense of the longer cable lengths required to connect every device on the LAN to one switch. This option should be compared with the cost of deploying a number of smaller switches connected by a few long cables to a central switch.

Deploying a number of smaller devices, instead of a single large device, also has the benefit of reducing the size of the ***failure domain***. A failure domain is the area of the network affected when a piece of networking equipment malfunctions or fails.

After the LAN switches are selected, determine which router is appropriate for the customer.

Refer to **Packet Tracer Activity** for this chapter

Packet Tracer Activity

Explore different LAN switch options.

3.3.4 Selecting Internetworking Devices

Refer to **Figure** in online course

A router is a Layer 3 device. It performs all tasks of devices in lower layers and selects the best route to the destination based on Layer 3 information. Routers are the primary devices used to interconnect networks. Each port on a router connects to a different network and routes packets between the networks. Routers have the ability to break up broadcast domains and collision domains.

When selecting a router, it is necessary to match the characteristics of the router to the requirements of the network. Factors for choosing a router include:

- Type of connectivity required
- Features available
- Cost

Connectivity

Routers interconnect networks that use different technologies. They can have both LAN and WAN interfaces.

The LAN interfaces of the router connect to the LAN media. The media is typically UTP cabling, but modules can be added for using fiber optics. Depending on the series or model of router, there can be multiple interface types for connecting LAN and WAN cabling.

Refer to **Figure** in online course

Features

It is necessary to match the characteristics of the router to the requirements of the network. After analysis, the business management may determine that it needs a router with specific features. In addition to basic routing, features include:

- Security
- Quality of Service (QoS)
- Voice over IP (VoIP)
- Network Address Translation (***NAT***)
- Dynamic Host Configuration Protocol (DHCP)
- Virtual Private Network (***VPN***)

Cost

Budget is an important consideration when selecting internetwork devices. Routers can be expensive, and additional modules, such as fiber optic modules, can increase the cost.

An Integrated Service Router (ISR) is a relatively new technology that combines multiple services into one device. Before the introduction of the ISR, multiple devices were required to meet the needs of data, wired, wireless, voice, video, firewall, and VPN technologies. The ISR was designed with multiple services to accommodate the demands of small- to medium-sized businesses

and branch offices of large organizations. With an ISR, an organization can quickly and easily enable end-to-end protection for users, applications, network endpoints, and wireless LANs. In addition, the cost of an ISR can be less than if the individual devices were purchased separately.

Refer to **Packet Tracer Activity** for this chapter

Packet Tracer Activity

Explore different internetworking device options.

3.3.5 Network Equipment Upgrades

Refer to **Figure** in online course

Many small networks were initially built using a low-end integrated router to connect wireless and wired users. These routers are designed to support small networks, usually consisting of a few wired hosts and possibly four or five wireless devices. When a small business outgrows the capabilities of their existing network devices, it is necessary to upgrade to more robust devices. Within this course, examples of these devices are the Cisco 1841 ISR and the Cisco 2960 Switch.

The Cisco 1841 is designed to be a branch office or medium-sized business router. As an entry-level multiservice router, it offers a number of different connectivity options. It is modular in design and can deliver multiple security services.

Refer to **Figure** in online course

Some of the features of the Catalyst 2960 switches are:

- Entry-level, enterprise-class, fixed-configuration switching that is optimized for Access Layer deployments
- Fast Ethernet and Gigabit Ethernet to desktop configurations
- Ideal for entry-level enterprise, mid-market, and branch-office environments
- Compact size for deployments outside of the wiring closet

These switches can provide the high speeds and high-density switching capabilities that the smaller ISRs with integrated switching cannot. They are a good option when upgrading networks built with either hubs or small ISR devices.

The Cisco Catalyst 2960 Series Intelligent Ethernet Switches are a family of fixed-configuration, standalone devices that provide Fast Ethernet and Gigabit Ethernet connectivity to the desktop.

3.3.6 Design Considerations

Refer to **Figure** in online course

Purchasing network devices and installing cables are only the beginning of the network upgrade process. Networks must also be reliable and available. Reliability can be achieved by adding redundant components to the network, such as two routers instead of one. In this instance, alternate data paths are created, so if one router is experiencing problems, the data can take an alternate route to arrive at the destination.

An increase in reliability leads to improved availability. For example, telephone systems require five-9s of availability. This means that the telephone system must be available 99.999% of the time. Telephone systems cannot be down, or unavailable, for more than .001% of the time.

Fault tolerance systems are typically used to improve network reliability. Fault tolerance systems include devices such as a UPS, multiple AC power supplies, hot-swappable devices, multiple interface cards, and backup systems. When one device fails, the redundant or backup system takes over to ensure minimal loss of reliability. Fault tolerance can also include backup communication links.

Refer to **Figure** in online course

IP Addressing Plan

Planning for a network installation must include planning the logical addressing. Changing the Layer 3 IP addressing is a major issue when upgrading a network. If the structure of the network is going to be changed in the upgrade, the IP address scheme and network information may need to be altered.

The plan should include every device that requires an IP address, and account for future growth. The hosts and network devices that require an IP address include:

- User computers
- Administrator computers
- Servers
- Other end devices such as printers, IP phones, and IP cameras
- Router LAN interfaces
- Router WAN (serial) interfaces

There are other devices that may need an IP address to access and manage them. These include:

- Standalone switches
- Wireless Access Points

For example, if a new router is introduced to the network, each interface on that router can be used to create additional networks, or subnets. These new subnets need to have the proper IP address and subnet mask calculated. Sometimes, this means having to assign a totally new addressing scheme to the network.

After all of the planning and design phases are complete, the upgrade proceeds to the implementation phase, in which the actual network installation begins.

Chapter Summary

Click through the buttons for summary information.

Go to the online course to take the quiz.

Chapter Quiz

Take the chapter quiz to check your knowledge.

Your Chapter Notes