Course Booklet

CCNA Discovery

Introducing Routing and Switching in the Enterprise

Version 4.0

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

CCNA Discovery Course Booklet Introducing Routing and Switching in the Enterprise, Version 4.0

Cisco Networking Academy

Copyright© 2010 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing October 2009

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

ISBN-13: 978-1-58713-256-8

ISBN-10: 1-58713-256-7

Warning and Disclaimer

This book is designed to provide information about routing and switching. 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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Course Introduction

Welcome

Welcome to the CCNA Discovery course, Introducing Routing and Switching in the Enterprise. The goal of this course is to assist you in developing the skills necessary to use protocols to maximize enterprise LAN and WAN performance. The course provides more advanced configurations of switching and routing protocols, configuration of access control lists, and basic implementation of WAN links. It also provides detailed troubleshooting guidance for LAN, WAN, and VLAN implementations. This course prepares you with the skills required for entry-level Network Technician, Help Desk Technician and Computer 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 2

Exploring the Enterprise Network Infrastructure

Introduction

2.1 Describing the Current Network

Refer to **Figure** in online course

2.1.1 Enterprise Network Documentation

Refer to **Figure** in online course

One of the first tasks for a new network technician is to become familiar with the current network structure. Enterprise networks can have thousands of hosts and hundreds of networking devices, all of which are interconnected by copper, fiber-optic, and wireless technologies. End-user workstations, servers, and networking devices, such as switches and routers, must all be documented. Various types of documentation show different aspects of the network.

Network infrastructure diagrams, or topology diagrams, keep track of the location, function, and status of devices. Topology diagrams represent either the physical or logical network.

A ***physical topology*** map uses icons to document the location of hosts, networking devices, and media. It is important to maintain and update physical topology maps to aid future installation and troubleshooting efforts.

A ***logical topology*** map groups hosts by network usage, regardless of physical location. Host names, addresses, group information, and applications can be recorded on the logical topology map. Connections between multiple sites may be shown but do not represent actual physical locations.

Enterprise network diagrams may also include control plane information. Control plane information describes failure domains and defines the interfaces where different network technologies intersect.

Refer to **Figure** in online course

It is crucial that network documentation remain current and accurate. Network documentation is usually accurate at the installation of a network. As the network grows or changes however, the documentation is not always updated.

Network topology maps are frequently based on original floor plans. The current floor plans may have changed since the construction of the building. Blueprints can be marked up, or ***redlined***, to show the changes. The modified diagram is known as an ***as-built***. An as-built diagram documents how a network was actually constructed which may differ from the original plans. Always ensure that the current documentation reflects the as-built floor plan and all network topology changes.

Network diagrams are commonly created using graphical drawing software. In addition to being a drawing tool, many network diagramming tools are linked to a database. This feature allows the network support staff to develop detailed documentation by recording information about hosts and networking devices, including manufacturer, model number, purchase date, warranty period, and more. Clicking a device in the diagram opens an entry form with device data listed.

Refer to **Figure** in online course

In addition to network diagrams, several other important types of documentation are used in the enterprise network.

Business Continuity Plan:

The Business Continuity Plan (***BCP***) identifies the steps to be taken to continue business operation in the event of a natural or man-made disaster.

Business Security Plan:

The Business Security Plan (***BSP***) includes physical, system, and organizational control measures. The overall security plan must include an IT portion that describes how an organization protects its network and information assets.

Network Maintenance Plan:

The Network Maintenance Plan (***NMP***) ensures business continuity by keeping the network up and running efficiently. Network maintenance must be scheduled during specific time periods, usually nights and weekends, to minimize the impact on business operations.

Service Level Agreement:

A Service Level Agreement (***SLA***) is a contractual agreement between the customer and a service provider or ISP, specifying items such as network availability and service response time.

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

Full Screen Activity

2.1.2 Network Operations Center (NOC)

Refer to **Figure** in online course

Most enterprise networks have a Network Operations Center (***NOC***) that allows for central management and monitoring of all network resources. The NOC is sometimes referred to as a ***Data Center***.

Employees in a typical enterprise NOC provide support for both local and remote locations, often managing both local and wide area networking issues. Larger NOCs may be multi-room areas of a building where network equipment and support staff are concentrated.

The NOC usually has:

- Raised floors to allow for cabling and power to run under the floor to the equipment
- High performance UPS systems and air conditioning equipment to provide a safe operating environment for equipment
- Fire suppression systems integrated into the ceiling
- Network monitoring stations, servers, backup systems, and data storage
- Access layer switches and distribution layer routers, if it serves as a Main Distribution Facility (MDF) for the building or campus where it is located

Refer to **Figure** in online course

In addition to providing network support and management, many NOCs also provide centralized resources such as servers and data storage.

Servers in the NOC are usually clustered together, creating a server farm. The ***server farm*** is frequently considered as a single resource but, in fact, provides two functions: backup and ***load balancing***. If one server fails or becomes overloaded, another server takes over.

The servers in the farm may be rack-mounted and interconnected by very high-speed switches (Gigabit Ethernet or higher). They may also be blade servers mounted in a chassis and connected by a high-speed backplane within the chassis.

Another important aspect of the enterprise NOC is high-speed, high-capacity data storage. This data storage, or network attached storage (***NAS***), groups large numbers of disk drives that are directly attached to the network and can be used by any server. A NAS device is typically attached to an Ethernet network and is assigned its own IP address.

A more sophisticated version of NAS is Storage Area Network (***SAN***). A SAN is a high-speed network that interconnects different types of data storage devices over a LAN or WAN.

Refer to **Figure** in online course

Equipment in the enterprise NOC is usually mounted in racks. In large NOCs, racks are usually floor-to-ceiling mounted and may be attached to each other. When mounting equipment in a rack, ensure there is adequate ventilation and access from front and back. Equipment must also be attached to a known good ground.

The most common rack width is 19 inches (48.26 cm). Most equipment is designed to fit this width. The vertical space that the equipment occupies is measured in Rack Units (***RU***s). A Unit equals 1.75 inches (4.4cm). For example, a 2U chassis is 3.5 inches (8.9 cm) high. The lower the RU number the less space a device needs therefore more devices can fit into the rack.

Another consideration is equipment with many connections, like switches. They may need to be positioned near patch panels and close to where the cabling is gathered into cable trays.

Refer to **Figure** in online course

In an enterprise NOC, thousands of cables may enter and exit the facility. ***Structured cabling*** creates an organized cabling system that is easily understood by installers, network administrators, and any other technicians who work with cables.

Cable management serves many purposes. First, it presents a neat and organized system that aids in isolating cabling problems. Second, best cabling practices protect the cables from physical damage and ***EMI***, which greatly reduces the number of problems experienced.

To assist in troubleshooting:

- All cables should be labelled at both ends, using a standard convention that indicates source and destination.
- All cable runs should be documented on the physical network topology diagram.
- All cable runs, both copper and fiber, should be tested end-to-end by sending a signal down the cable and measuring loss.

Cabling standards specify a maximum distance for all cable types and network technologies. For example, the IEEE specifies that, for Fast Ethernet over unshielded twisted pair (UTP), the cable run from switch to host cannot be greater than 100 meters (approximately 328 ft). If the cable run is greater than the recommended length problems could occur with data communications, especially if the terminations at the ends of the cable are poorly completed.

Documentation of the cable plan and testing are critical to network operations.

2.1.3 Telecommunication Room Design and Considerations

Refer to **Figure** in online course

The NOC is the central nervous system of the enterprise. In practice, however, most users connect to a switch in a ***telecommunications room***, which is some distance from the NOC. The telecommunications room is also referred to as a wiring closet or intermediate distribution facility (***IDF***). It contains the Access Layer networking devices and ideally maintains environmental conditions similar to the NOC, such as air conditioning and UPS.

Users working with wired technology connect to the network through Ethernet switches or hubs. Users working with wireless technology connect through an access point (***AP***). Access Layer devices such as switches and APs are a potential vulnerability in network security. Physical and remote access to this equipment should be limited to authorized personnel only. Network personnel can also implement port security and other measures on switches, as well as various wireless security measures on APs.

Securing the telecommunications room has become even more important because of the increasing occurrence of identity theft. New privacy legislation results in severe penalties if confidential data from a network falls into the wrong hands. Modern networking devices offer capabilities to help prevent these attacks and protect data and user integrity.

Refer to **Figure** in online course

Many IDFs connect to a Main Distribution Facility (***MDF***) using an ***extended star*** design. The MDF is usually located in the NOC or centrally located within the building.

MDFs are typically larger than IDFs. They house high-speed switches, routers, and server farms. The central MDF switches may have enterprise servers and disk drives connected using gigabit copper links.

IDFs contain lower-speed switches, APs, and hubs. The switches in the IDFs typically have large numbers of Fast Ethernet ports for users to connect at the Access Layer.

The switches in the IDF usually connect to the switches in the MDF with Gigabit interfaces. This arrangement creates backbone connections, or uplinks. These backbone links, also called vertical cabling, may be copper or fiber-optic. Copper Gigabit or Fast Ethernet links are limited to a maximum of 100 meters and should use CAT5e or CAT6 UTP cable. Fiber-optic links can run much greater distances. Fiber-optic links commonly interconnect buildings and because they do not conduct electricity, they are immune to lightning strikes, EMI, RFI, and differential grounds.

Refer to **Figure** in online course

In addition to providing basic network access connectivity, it is becoming more common to provide power to end-user devices directly from the Ethernet switches in the telecommunications room. These devices include IP phones, access points, and surveillance cameras.

These devices are powered using the IEEE 802.3af standard, Power over Ethernet, or ***PoE***. PoE provides power to a device over the same twisted pair cable that carries data. This allows an IP phone, for instance, to be located on a desk without the need for a separate power cord or a power outlet. In order to support PoE devices such as the IP phone, the connecting switch must have PoE capability.

PoE can also be provided by power injectors or PoE patch panels for those switches which do not support PoE. Panduit and other suppliers produce PoE patch panels that allow non PoE capable switches to participate in PoE environments. Legacy switches connect into the PoE patch panel which then connects to the PoE capable device.

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

Activity

Place the MDF and IDFs in an appropriate location in the campus diagram and identify appropriate cables to connect them.

2.2 Supporting the Enterprise Edge

2.2.1 Service Delivery at the Point-of-Presence

Refer to **Figure** in online course

At the outer edge of the enterprise network is the Point-of-Presence (***POP***) which provides an entry point for services to the enterprise network. Externally-provided services coming in through the POP include Internet access, wide area connections, and telephone services (PSTN).

The POP contains a point of demarcation, or the ***demarc***. The demarc provides a boundary that designates responsibility for equipment maintenance and troubleshooting between the service provider (***SP***) and customer. Equipment from the service provider up to the point of demarcation is the responsibility of the provider; anything past the demarc point is the responsibility of the customer.

In an enterprise, the POP provides links to outside services and sites. The POP may provide a direct link to one or more ISPs, which allows internal users the required access to the Internet. The remote sites of an enterprise are also interconnected through the POPs. The service provider establishes the wide area links between these remote sites.

The location of the POP and the point of demarcation vary in different countries. While they are often located within the MDF of the customer, they may also be located at the ISP.

2.2.2 Security Considerations at the Enterprise Edge

Refer to **Figure** in online course

Large enterprises usually consist of multiple sites that interconnect. Multiple locations may have edge connections at each site connecting the enterprise to other individuals and organizations.

The edge is the point of entry for outside attacks and is a point of vulnerability. Attacks at the edge can affect thousands of users. For example, Denial of Service (***DoS***) attacks prevent access to resources for legitimate users inside or outside the network, affecting productivity for the entire enterprise.

All traffic in or out of the organization goes through the edge. Edge devices must be configured to defend against attacks and provide filtering based on website, IP address, traffic pattern, application, and protocol.

An organization can deploy a ***firewall***, and security appliances with intrusion detection system (IDS) and intrusion prevention system (IPS) at the edge to protect the network.

External network administrators require access for internal maintenance and software installation. Virtual private networks (VPNs), access control lists (ACLs), user IDs, and passwords provide that access. VPNs also allow remote workers access to internal resources.

2.2.3 Connecting the Enterprise Network to External Services

Refer to **Figure** in online course

The network connection services commonly purchased by an enterprise include leased lines, ***T1***/***E1*** or business class, Frame Relay, and ATM. Physical cabling brings these services to the enterprise using copper wires, as in the case of T1/E1, or fiber-optic cable for higher-speed services.

The POP must contain certain pieces of equipment to obtain whichever WAN service is required. For example, to obtain T1/E1 service, the customer may require a ***punchdown block*** to terminate the T1/E1 circuit, as well as a Channel Service Unit / Data Service Unit (***CSU/DSU***) to provide the proper electrical interface and signaling for the service provider. This equipment may be owned and maintained by the service provider or may be owned and maintained by the customer. Regardless of ownership, all equipment located within the POP at the customer site is referred to as Customer Premise Equipment (***CPE***).

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

Activity

Specify the components, in the correct sequence needed to connect a service from the edge to the internal network.

2.3 Reviewing Routing and Switching

2.3.1 Router Hardware

Refer to **Figure** in online course

One important device in the ***Distribution Layer*** of an enterprise network is a router. Without the routing process, packets could not leave the local network.

The router provides access to other private networks as well as to the Internet. All hosts on a local network specify the IP address of the local router ***interface*** in their IP configuration. This router interface is the ***default gateway***.

Routers play a critical role in networking by interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols. For example, a router can re-encapsulate packets from an Ethernet to a Serial encapsulation.

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link goes down or traffic is congested.

Routers also serve other beneficial functions:

- Provide broadcast containment
- Connect remote locations
- Group users logically by application or department
- Provide enhanced security (using NAT and ACLs)

With the enterprise and the ISP, the ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Refer to **Figure** in online course

Routers come in many shapes and sizes called ***form factor***s. Network administrators in an enterprise environment should be able to support a variety of routers and switches, from a small desktop to a rack-mounted or blade model.

Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built-in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. As an example, a Cisco 1841 router comes with two Fast Ethernet RJ-45 interfaces built-in, and two slots that can accommodate many different network interface modules.

Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic. Router interfaces use the controller/interface or controller/slot/interface conventions. For example, using the controller/interface convention, the first Fast Ethernet interface on a router is numbered as Fa0/0 (controller 0 and interface 0). The second is Fa0/1. The first serial interface on a router uses controller/slot/interface is S0/0/0.

Refer to **Figure** in online course

Two methods exist for connecting a PC to a network device for configuration and monitoring tasks: ***out-of-band*** and ***in-band*** management.

Out-of-band management is used for initial configuration or when a network connection is unavailable. Configuration using out-of-band management requires:

- Direct connection to console or AUX port
- Terminal emulation client

In-band management is used to monitor and make configuration changes to a network device over a network connection. Configuration using in-band management requires:

- At least one network interface on the device to be connected and operational
- Telnet, SSH, or HTTP to access a Cisco device

2.3.2 Basic Router CLI Show Commands

Refer to **Figure** in online course

Here are some of the most commonly used IOS commands to display and verify the operational status of the router and related network functionality. These commands are divided into several categories.

General Use:

- `show running-config`
- `show startup-config`
- `show version`

Routing Related:

- `show ip protocols`
- `show ip route`

Interface Related:

- `show interfaces`
- `show ip interface brief`
- `show protocols`

Connectivity Related:

- `show cdp neighbors`
- `show sessions`
- `show ssh`
- `ping`
- `traceroute`

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

Full Screen Activty

2.3.3 Basic Router Configuration Using CLI

Refer to **Figure** in online course

A basic router configuration includes the hostname for identification, passwords for security, and assignment of IP addresses to interfaces for connectivity. Verify and save configuration changes using the **`copy running-config startup-config`** command. To clear the router configuration, use the **`erase startup-config`** command and then the **`reload`** command.

Configuration Management:

- `enable`

- `configure terminal`
- `copy running-config startup-config`
- `erase startup-config`
- `reload`

Global Settings:

- `hostname`
- `banner motd`
- `enable password`
- `enable secret`

Line Settings:

- `line con`
- `line aux`
- `line vty`
- `login and password`

Interface Settings:

- `interface type/number`
- `description`
- `ip address`
- `no shutdown`
- `clock rate`
- `encapsulation`

Routing Settings:

- `router`
- `network`
- `ip route`

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

Packet Tracer Activity

Practice basic router configuration and verification commands.

2.3.4 Switch Hardware

Refer to **Figure** in online course

Although all three layers of the hierarchical design model contain switches and routers, the Access Layer generally has more switches. The main function of switches is to connect hosts such as end user workstations, servers, IP phones, web cameras, access points and routers. This means that there are many more switches in an organization than routers.

Switches come in many form factors:

- Small standalone models sit on a desk or mount on a wall.

Refer to **Figure** in online course

- Integrated routers include a switch built into the chassis that is rack mounted.
- High-end switches mount into a rack and are often a chassis and blade design to allow more blades to be added as the number of users increases.

High-end enterprise and service provider switches support ports of varying speeds, from 100 MB to 10 GB.

An enterprise switch in an MDF connects other switches from IDFs using Gigabit fiber or copper cable. An IDF switch typically needs both RJ-45 Fast Ethernet ports for device connectivity and at least one Gigabit Ethernet port (copper or fiber) to uplink to the MDF switch. Some high-end switches have modular ports that can be changed if needed. For example, it might be necessary to switch from multimode fiber to single mode fiber, which would require a different port.

Like routers, switch ports are also designated using the controller/port or controller/slot/port conventions. For example, using the controller/port convention, the first Fast Ethernet port on a switch is numbered as Fa0/1 (controller 0 and port 1). The second is Fa0/2. The first port on a switch that uses controller/slot/port is Fa0/0/1. Gigabit ports are designated as Gi0/1, Gi0/2 etc.

Port density on a switch is an important factor. In an enterprise environment where hundreds or thousands of users need switch connections, a switch with a 1RU height and 48-ports has a higher port density than a 1RU 24-port switch.

2.3.5 Basic Switch CLI Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status. These commands can be divided into several categories, as follows:

Refer to **Figure** in online course

General Use:

- `show running-config`
- `show startup-config`
- `show version`

Interface / Port Related:

- `show interfaces`
- `show ip interface brief`
- `show port-security`
- `show mac-address-table`

Connectivity Related:

- `show cdp neighbors`
- `show sessions`
- `show ssh`
- `ping`
- `traceroute`

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

The same in-band and out-of-band management techniques that apply to routers also applies to switch configuration.

Full screen activity

Refer to **Figure** in online course

A basic switch configuration includes the hostname for identification, passwords for security, and assignment of IP addresses for connectivity. In-band access requires the switch to have an IP address.

Verify and save the switch configuration using the **copy running-config startup-config** command. To clear the switch configuration, use the **erase startup-config** command and then the **reload** command. It may also be necessary to erase any VLAN information using the command **delete flash:vlan.dat**.

Configuration Management:

- **enable**
- **configure terminal**
- **copy running-config startup-config**
- **erase startup-config**
- **delete flash:vlan.dat**
- **reload**

Global Settings:

- **hostname**
- **banner motd**
- **enable password**
- **enable secret**
- **ip default-gateway**

Line Settings:

- **line con**
- **line vty**
- **login and password**

Interface Settings:

- **interface type/number (vlan1)**
- **ip address**
- **speed / duplex**
- **switchport port-security**

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

Packet Tracer Activity

Configure a switch in a switching environment.

Refer to **Lab Activity** for this chapter

Lab Activity

Connect and configure a multi-router network.

Summary

Go to the online course to take the quiz.

Quiz

Take the chapter quiz to check your knowledge.

Your Chapter Notes