



CISCO NETWORKING ACADEMY PROGRAM



# CCNA 2:

## Routers and Routing Basics v3.1

### Instructor Guide

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for noncommercial distribution and exclusive use by instructors in the CCNA 2: Routers and Routing Basics course as part of an official Cisco Networking Academy Program.



# I. Welcome

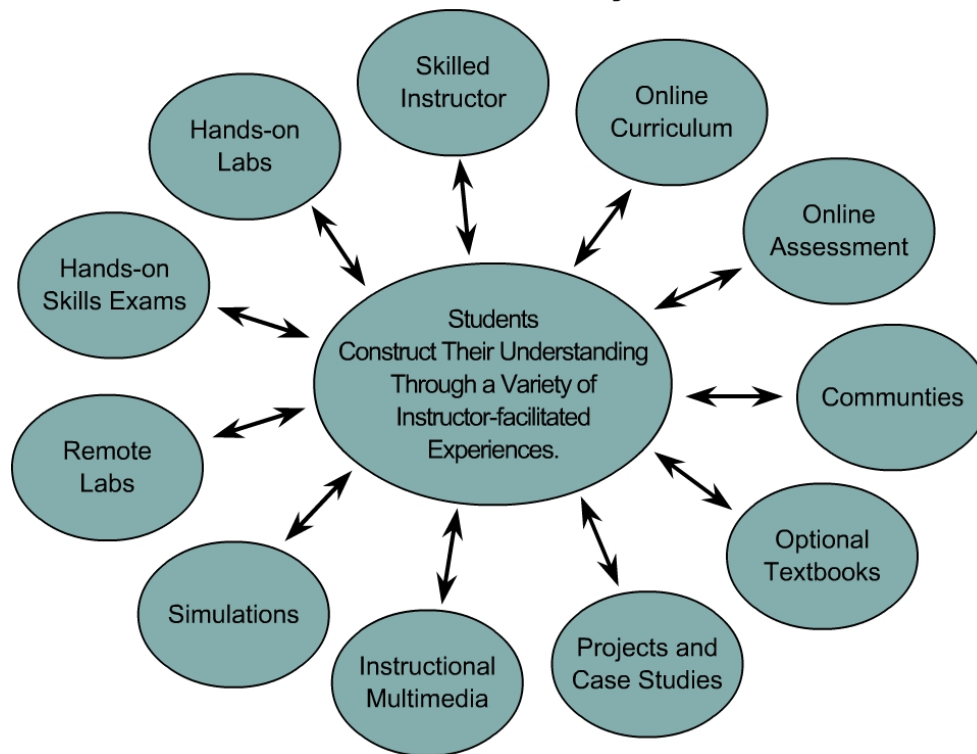
Welcome to the CCNA 2 version 3.1 Instructor Guide. Cisco Worldwide Education (WWE) has developed this guide to provide a helpful resource for instructors. This introduction will emphasize four themes:

- Student-centered, instructor-facilitated model
- One size does not fit all
- Hands-on, skills-based learning
- Global community of educators

## Student-Centered, Instructor-Facilitated

The CCNA curriculum has not been designed as a standalone e-learning or distance-learning course. The teaching and learning model of the Cisco Networking Academy® Program is based on instructor facilitation. The Learner Model: Academy Student diagram shows the emphasis that WWE puts on the learner. The model begins with the prior knowledge of students. The instructor guides learning events, which are built from a variety of resources, to help the students achieve their desired comprehension of networking.

### Learner Model: Academy Student



## One Size Does Not Fit All

The Cisco Networking Academy Program serves hundreds of thousands of students in almost 150 countries. Students range from early teens to mature adults and from advanced middle school students to undergraduate engineering students.

One curriculum cannot fit the needs of all students. WWE relies on local instructors to make the program work and to help their students achieve the learning goals of the program. There are three fixed reference points for each program that provide flexibility for the instructors:

- The mission of WWE to educate and train
- The requirements of the CCNA certification exam
- The hands-on skills that help prepare students for the industry and further education

The WWE policy allows instructors to "add anything, but subtract nothing" from the curriculum. WWE supports in-class differentiation, which is used to provide additional support for students who need it and additional challenges for advanced students. WWE also allows instructors to decide how much time to spend on various topics. Some topics can be skimmed, while others may need to be emphasized for different audiences. The local instructor must decide how to balance the need for hands-on labs with the realities of the local student-to-equipment ratio and time schedule. This Guide can be used to facilitate the preparation of lesson plans and presentations. Instructors are encouraged to research and use external sources to develop additional labs and exercises.

Core TIs have been highlighted for emphasis to assist the instructor in course and lesson planning. These are not the only TIs that need to be taught. Many core TIs will only make sense after the preceding TIs have been reviewed. It may be useful to have a map of the core TIs, which contain the most important knowledge and skills for success in the CCNA program.

The assessment process is multifaceted and flexible. A wide variety of assessment options exist to provide feedback to students and document their learning. The Academy assessment model is a blend of formative and summative assessments that include online and hands-on, skills-based exams.

## Hands-On, Skills-Based

The core of the CCNA 2 experience is the sequence of hands-on labs. Labs are designated as either essential or optional. Essential labs include information that is fundamental to the CCNA Academy student experience. This information will help students prepare for the certification exam, succeed in job situations, and develop their cognitive abilities. In CCNA 2, students will learn about the following elements of basic router configuration:

- Hostnames, banners, and passwords
- Interface configuration
- IOS file system
- Static routes and dynamic routing (RIP version 1 and IGRP)

- Standard and extended access-list configuration and placement
- `show`, `debug`, `ping`, `trace`, and `telnet` commands to verify and troubleshoot

## **Global Community**

WWE instructors are members of a global community of educators. There are over 10,000 instructors that teach the same eight CCNA and CCNP courses in the program. Instructors should take advantage of the diversity and skills of this community through their Regional Academies, Cisco Academy Training Centers (CATCs), the Cisco Academy Connection (CAC), or through other forums. WWE is committed to the improvement of the curriculum, assessment model, and instructional resources such as this guide. Please submit any feedback through CAC. Check CAC for new releases of instructional materials.

## **Guide Overview:**

Section II provides a scope and sequence overview of the course. Section III summarizes the most important learning objectives, target indicators, and labs, and offers teaching suggestions and background information. Section IV provides a case study related to network design, implementation, and troubleshooting. Instructors can also devise their own case studies. Section V includes four appendices:

- Cisco online tools and utilities
- CCNA assessment guidelines
- Evidence-centered design of assessment tasks in the Networking Academy program
- Instructional best practices

## II. Course Overview

### Target Audience

The target audience is anyone who desires a practical and technical introduction to the field of networking. This includes high school, community college, and lifelong-learning students who are interested in careers as network technicians, network engineers, network administrators, and network help-desk staff.

### Prerequisites

The successful completion of this course requires the following:

- Reading age level of 13 or higher
- Successful completion of CCNA 1

The following prerequisites are beneficial, but not required:

- Prior experience with computer hardware and command line interfaces
- Background in computer programming

### Course Description

CCNA 2: Routers and Routing Basics is the second of four CCNA courses that lead to the Cisco Certified Network Associate (CCNA) designation. CCNA 2 focuses on initial router configuration, Cisco IOS Software management, routing protocol configuration, TCP/IP, and access control lists (ACLs). Students will learn how to configure a router, manage Cisco IOS software, configure routing protocols on routers, and set access lists to control access to routers.

### Course Objectives

The CCNA certification indicates knowledge of networking for the small office, home office (SOHO) market and the ability to work in small businesses or organizations that use networks with fewer than 100 nodes. A CCNA-certified individual can perform the following tasks:

- Install and configure Cisco switches and routers in multiprotocol internetworks that use LAN and WAN interfaces
- Provide Level 1 troubleshooting service
- Improve network performance and security
- Perform entry-level tasks in the planning, design, installation, operation, and troubleshooting of Ethernet and TCP/IP Networks

Students must successfully complete the CCNA 2 course before they can achieve CCNA certification.

Upon completion of this course, students will be able to perform tasks related to the following:

- Routers and their roles in WANs
- Cisco IOS Software Management
- Router configuration
- Router file management
- RIP and IGRP routing protocols
- TCP/IP error and control messages
- Router troubleshooting
- Intermediate TCP
- Access control lists

## Lab Requirements

Please refer to the CCNA equipment bundle spreadsheets on the Cisco Academy Connection.

## Certification Alignment

The curriculum is aligned with the following Cisco Internet Learning Solution Group (ILSG) courses:

- CCNA (Cisco Certified Network Associate)
- INTRO (Introduction to Cisco Networking Technologies)

The Course 2 claims state that students will be able to complete the following tasks:

- Identify the key characteristics of common wide-area network (WAN) configurations and technologies, and differentiate between these and common LAN technologies
- Describe the role of a router in a WAN
- Describe the purpose and operations of the router Internet Operating System (IOS)
- Establish communication between a terminal device and the router IOS, and use IOS for system analysis, configuration, and repair
- Identify the major internal and external components of a router, and describe the associated functionality

- Connect router Fast Ethernet, serial WAN, and console ports
- Perform, save, and test an initial configuration on a router
- Configure additional administrative functionality on a router
- Use embedded data-link layer functionality to perform network neighbor discovery and analysis from the router console
- Use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console
- Identify the stages of the router boot-up sequence and show how the configuration register and boot system commands modify that sequence
- Manage system image and device configuration files
- Describe the operation of the Internet Control Message Protocol (ICMP) and identify the reasons, types, and format of associated error and control messages
- Identify, configure, and verify the use of static and default routes
- Evaluate the characteristics of routing protocols
- Identify, analyze, and show how to rectify inherent problems associated with distance vector routing protocols
- Configure, verify, analyze, and troubleshoot simple distance vector routing protocols
- Use commands incorporated within IOS to analyze and rectify network problems
- Describe the operation of the major transport layer protocols and the interaction and carriage of application layer data
- Identify the application of packet control through the use of various access control lists
- Analyze, configure, implement, verify, and rectify access control lists within a router configuration

## Course Overview

The course has been designed for 70 contact hours. Approximately 35 hours will be designated to lab activities and 35 hours will be designated to curriculum content. A case study on routing is required. The format and timing should be determined by the Local Academy.

The following changes have taken place since CCNA version 2.x:

- More emphasis on router configuration early in semester
- More efficient presentation and practice of IOS
- IGRP moved from CCNA 3 to CCNA 2
- Access lists moved from CCNA 3 to CCNA 2
- Revisions to TCP/IP coverage
- More focus on routing tables
- Case study is required with format and timing determined by the Local Academy
- More interactive flash activities
- Sequence of over 40 e-Labs
- Lab focus on two-router labs



# III. Teaching Guide for Each TI

## Nomenclature

The CCNA curriculum uses the following hierarchy:

- Course
- Module
- Learning objective (LO)
- Target indicator (TI)

For example, 3.2.5 references Module 3, LO 2, and TI 5. The following terms are commonly used to describe the curriculum, instructional materials, and assessments in WWE and Cisco documentation:

- **Certification-level claims**

High-level statements about what a CCNA-certified person should know and be able to do. These claims are measured through certification exams.

- **Course**

A subset of a curriculum which is a collection of chapters to be offered as a scheduled course.

- **Course-level claims**

Medium-level statements about what a person who completes the CCNA 2 course should know and be able to do.

- **Core TI**

The TIs that apply most directly to the claims and learning objectives. Instructors should not skip over these TIs or move through them quickly.

- **Curriculum**

A predefined or dynamic path of learning events with an end goal such as certification or the acquisition of required job skills and knowledge.

- **Hands-on skills**

There is some overlap between hands-on skills and claims. These statements emphasize hands-on, lab-based learning.

- **Module**

Logical groupings that comprise a course. Modules contain multiple lessons or LOs. Modules are also referred to as chapters.

- **Learning objective (LO)**

A statement that establishes a measurable behavioral outcome. LOs are used to organize content and to indicate how the acquisition of skills and knowledge will be measured. LOs are also referred to as terminal objectives or RLOs.

- **Lesson**

A set of TIs, or enabling objectives, that are grouped together and presented in a coherent format to meet an LO, or terminal objective. Lessons emphasize the role of the instructor. Learning objectives emphasize the role of the students.

- **Module caution**

Suggestions related to areas where difficulties may be encountered. These are especially important for syllabus development, lesson planning, and pacing.

- **Optional lab**

A lab that is for practice, enrichment, or differentiation.

- **Essential lab**

A lab that is fundamental to the course.

- **Reusable Learning Object (RLO)**

This is a Cisco Instructional Design term. RLOs typically consist of five to nine RIOs. In this guide, RLOs are equivalent to lessons or learning objectives.

- **Reusable Information Object (RIO)**

This is a Cisco Instructional Design term. In this guide, RIOs are equivalent to target indicators.

- **Target indicator (TI)**

TIs are also referred to as enabling objectives or RIOs. TIs typically consist of a text frame with graphics and several media content items.

# Module 1: WANs and Routers

## Overview

When teaching Module 1, show the students how router configuration relates to the Internet, which is a global internetwork made possible by routers. Students will learn the difference between WANs and LANs, and will identify WAN connections, encapsulations, and protocols.

### Module 1 Caution

WANs will be taught in detail in CCNA 4. In CCNA 2, it is important to teach students the fundamental basics of WANs and roles that routers play in the WAN connection. Inform the students that the serial interfaces will be used to simulate the DCE to DTE WAN connection. Do not spend too much time on this module.

Students who complete this module should be able to:

- Identify organizations responsible for WAN standards
- Explain the difference between WANs and LANs and the types of addresses they use
- Describe the role of a router in a WAN
- Identify internal components of a router and describe their functions
- Describe the physical characteristics of a router
- Identify common ports on a router
- Connect Ethernet, serial WAN, and console ports

## 1.1 WANs

**Essential labs:** None

**Optional labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-level claim:** Students can identify the important characteristics of common WAN configurations and technologies, differentiate between these and common LAN technologies, and describe the role of a router in a WAN.

**Certification-level claim:** Students can evaluate the important characteristics of WANs and implement simple WAN protocols.

**Hands-on skills:** none

### 1.1.1 Introduction to WANs

WANs differ from LANs in several ways:

- LANs connect workstations, peripherals, terminals, and other devices in a single building or several buildings that are located next to each other, and WANs connect large geographic areas.
- LANs connect devices and WANs connect data connections across a broad geographic area.

WANs operate at the physical and data-link layers of the OSI model. Devices used in a WAN are routers, switches, modems, and communication servers. The following topics are relevant to this TI:

- Discuss the various carriers and devices available for WAN connections.
- Show students what routers in a WAN look like.
- Explain what routers do.

Figure 3 is an important figure to review. Best instructional practices for this TI include online study sessions with study guides, group work, and mini-lectures. This TI provides essential background information for the CCNA exam.

### 1.1.2 Introduction to routers in a WAN

Routers and computers have four basic common components:

- CPU
- Bus

- Memory
- Interfaces

However, the main purpose of a router is to route, not to compute. The main components of the router are as follows:

- RAM
- NVRAM
- Flash
- ROM
- Interfaces

The following topics should be covered in this TI:

- Discuss the similarities of computers and routers such as the software they use.
- Explain the components of the router and what each component contains.
- Open a router and let the students examine the inside. Point out the main components.
- Explain that just as a computer cannot work without an operating system and software, a router cannot work without an operating system and configurations.

### 1.1.3 Router LANs and WANs

Routers function in both LANs and WANs. They are primarily used in WANs. Explain that routers have both LAN and WAN interfaces. Students should be able to identify the differences. The two main functions of a router are to select the best path and to forward packets to the correct outgoing interfaces.

Networking models are useful because they facilitate modularity, flexibility, and adaptability. Like the OSI model, the three-layer design model is an abstract picture of a network. Models may be difficult to comprehend because the exact composition of each layer varies from network to network.

Explain that each layer of a three-layer design model may include a router, a switch, a link, or some combination of these. Some networks may combine the function of two layers into a single device or may omit a layer entirely. The three-layer design model consists of the following:

- The core layer forwards packets as quickly as possible.
- The distribution layer provides a boundary by using filters to limit what gets to the core.
- The access layer feeds traffic into the network and controls entry into the network.

### 1.1.4 Role of Routers in a WAN

There are several encapsulations associated with serial lines:

- HDLC
- Frame Relay
- PPP
- SDLC
- SLIP
- LAPB

Some of the most common WAN technologies are as follows:

- POTS
- ISDN
- X.25
- Frame Relay
- ATM
- T1, T3, E1, and E3
- DSL
- SONET

Ask students to briefly explain each of the WAN technologies and discuss the differences between technologies and encapsulations. They will be covered in detail in CCNA 4.

It is important to encourage student interest and enthusiasm in this TI. The world of WAN technologies is briefly introduced. Many students will be familiar with one or more of the technologies used. Many of these topics will be covered in CCNA 4 and students should be encouraged to do additional research on one of these technologies and present it to the class.

### 1.1.5 Academy approach to hands-on labs

In the Networking Academy lab, all the networks are connected with a serial or Ethernet cable. This allows the students to see and touch all of the equipment. In a real network, the routers would not be in one physical location. In the Networking Academy lab, the serial cables are connected back-to-back. However, in the real world the cables would be connected through a CSU or DCE device.

Discuss the differences between real networking environments and the router lab setup. Help the students visualize the components between the V.35 connectors. If they can understand this picture, then they will realize that they are working with a complete WAN minus the carrier services.

Each student should build a complete topology and then take it apart and let the next student do the lab. These labs are a review of the cabling labs in CCNA 1. This may be one of the last opportunities students have to cable a network, so do not miss this opportunity to make sure students complete the CCNA 2 Lab setup. This is a good place to introduce troubleshooting and the Layer 1 issues that occur in CCNA 2. It is also a fairly simple and fun activity.

## 1.2 Routers

**Essential Labs:** 1.2.5, 1.2.6, and 1.2.7

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course- Level Claim:** Students can properly connect router Fast Ethernet, Serial WAN, and console ports.

**Certification-Level Claim:** Students can describe the components of network devices. They can also identify the major internal and external components of a router and describe the associated functionality.

**Hands-on skills:** none

### 1.2.1 Introduction to WANs

This section overviews the physical aspect of a router. The physical layer is always studied first in networking topics. The student will be able to identify internal components of the router and describe their functions, describe the physical characteristics of the router, identify common ports on a router, and properly connect FastEthernet, Serial WAN, and console ports.

The components in a router are essentially the same as those in a computer. In fact, a router can be thought of as a computer designed for the special purpose of routing. While the exact architecture of the router varies in different router series, this section will introduce the major internal components. The figures show the internal components of some of the Cisco router models.

Ask students the following questions:

- What are the common components of a router?
- What is NVRAM used for?

### 1.2.2 Router physical characteristics

It is not necessary to know the location of the physical components inside the router to understand how to use the router. The exact components used and their locations vary in different router models.

Ask students the following questions:

- What are the different types of RAM used by a router?
- Can the RAM be upgraded in a router?

### 1.2.3 Router external connections

The three basic types of connections on a router are LAN interfaces, WAN interfaces, and management ports. LAN interfaces allow the router segment network boundaries within a LAN and reduce broadcast traffic within a LAN. WAN connections are provided through a service provider which connects two or more distant site through the Internet or PSTN. The LAN and WAN connections provide network connections through which frames are passed. The management port provides an ASCII or text-based connection for the configuration and troubleshooting of the router.

Ask students the following questions:

- What are the three basic types of connections on a router?
- What is the console connection used for?

### 1.2.4 Management port connections

The management ports are asynchronous serial ports. They are the console port and the auxiliary port. Not all routers have an auxiliary port. These serial ports are not designed as networking ports. To prepare for initial startup and configuration, attach an RS-232 ASCII terminal or a computer that emulates an ASCII terminal to the system console port.

It is essential for students to understand the difference between network interfaces and non-network interfaces. The instructor may need to talk about the differences extensively.

Discuss the following topics:

- The network ports use network encapsulation frames while the non-network ports are bit and byte oriented.
- There is no addressing involved in the serial management ports.
- The serial interface for management is asynchronous and the serial WAN interface is synchronous.

Ask students the following questions:

- Which port is preferred for troubleshooting and why?
- Do all routers have an auxiliary port?

### 1.2.5 Console Port Connections

The console port is a management port used to provide out-of-band access to a router. It is used for the initial configuration of the router, monitoring, and disaster recovery procedures.



Students may not be familiar with the term out-of-band. Out-of-band refers to the fact that the management control communications use a different path or channel than the data communications.

Ask students the following questions:

- What type of terminal emulation must the PC or terminal support?
- What are the steps to connect the PC to a router?

### 1.2.6 Connecting Router LAN interfaces

In most LAN environments, an Ethernet or FastEthernet interface is used to connect the router to the LAN. The router is a host that connects to the LAN through a hub or a switch. A straight-through cable is used to make this connection. The correct interface must be used.

If the wrong interface is connected, the router or other networking devices may be damaged. This is generally not true within LAN interfaces. However, if LAN interfaces are connected to some form of WAN interface such as ISDN, damage can occur. The students should be taught to be observant and careful whenever connections are made.

Ask students the following questions:

- What type of cable is used to connect from the router Ethernet interface to a hub or switch?
- What type of cable is used to connect from the router Ethernet interface to a router Ethernet interface?

### 1.2.7 Connecting WAN interfaces

There are many forms of WAN connections. A WAN uses many different types of technology to make data connections across a broad geographic area. WAN services are usually leased from service providers. The WAN connection types include leased line, circuit switched, and packet switched.

Many of the WAN interfaces use the same physical interfaces but different pinouts and electrical characteristics. This difference in electrical characteristics could potentially cause damage if the wrong connections were made. Again, the students should be taught to be observant and careful when they make any connections.

Ask students to perform the following tasks:

- List the physical layer standards that Cisco routers support.
- List the different types of WAN connections.

## Module 1 Summary

Before students move on to Module 2, they must be able to cable the lab setup, identify all external relevant ports, and identify internal router components.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 1 exam. Consider introducing formative assessments, where the instructor supervises the students as they work on the router setup. The use of formative assessments can be very valuable while students work through this router-intensive and IOS-intensive course.

Students should understand the following main points:

- WAN and LAN concepts
- Role of a router in WANs and LANs
- WAN protocols
- How to configure console connections
- The identification and description of the internal components of a router
- The physical characteristics of a router
- The common ports on a router
- How to connect router console, LAN, and WAN ports

# Module 2: Introduction to Routers

## Overview

Consider the prior knowledge of students when teaching Module 2. Some students may be familiar with command-line interfaces (CLIs). Students who have only used GUIs may not know how to use CLIs to interact with a computer. Students should experiment with CLIs to learn how to interact with a router.

### Module 2 Caution

Students need to know what the IOS is and what it does. They also need to know the difference between the configuration file and the IOS. It is also important for students to feel comfortable when they enter into and move around in the CLI. Do not move too quickly through these labs. If students are uncomfortable with the CLI, they will have difficulties with more complex labs.

Students who complete this module should be able to perform the following tasks:

- Describe the purpose of the IOS
- Describe the basic operation of the IOS
- Identify various IOS features
- Identify the methods to establish a command-line interface (CLI) session with the router
- Move between the user command executive (EXEC) and privileged EXEC modes
- Establish a HyperTerminal session on a router
- Log into a router
- Use the help feature in the command-line interface
- Troubleshoot command errors

## 2.1 Operating Cisco IOS Software

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can describe the purpose and fundamental operation of the router IOS.

**Certification-Level Claim:** Students can establish communication between a terminal device and the router IOS and use it for system analysis, configuration, and repairs.

**Hands-on skills:** none

### 2.1.1 The purpose of Cisco IOS software

In this TI, students will be introduced to the fundamentals of the Cisco Internet Operating System (IOS). Student will learn about the `show version` command, which helps users gain information about the Cisco IOS. The IOS command line interface is introduced in another lesson, so there is no need to focus on the `show` command in this TI.

A router and switch cannot function without an operating system. Cisco IOS is the installed software in all Cisco routers and Catalyst switches.

A computer needs an operating system such as Windows or UNIX. Discuss how the hardware cannot function without this software. Make sure the students understand the role of the IOS.

### 2.1.2 Router user interface

Cisco IOS software uses a command-line interface (CLI) as its console environment. The CLI is accessible through several methods:

- Console port
- Auxiliary port
- Telnet session

Students should know the difference between these methods. They should also be comfortable with the term CLI.

### 2.1.3 Router user interface modes

The user EXEC mode allows a limited number of basic monitoring commands. This mode is often referred to as a view-only mode. The privileged EXEC mode provides access to all router commands. To enter the privileged mode from user mode the `enable` command must be entered. The privileged mode is used to access other modes to configure the router.

Students should be able to identify the router prompts. The user mode prompt is `Router>`. The privileged mode prompt is `Router#`.

### 2.1.4 Cisco IOS software features

Cisco IOS devices have three operating environments:

- ROM monitor
- Boot ROM
- Cisco IOS

ROM monitor is used to recover from system failures and recover a lost password. Boot ROM is used to modify the Cisco IOS image in flash. There is a limited subset of features in this mode. Normal operation of a router requires the full Cisco IOS image. Discuss the three operating environments. Students should be able to identify these environments. Students must be familiar with the IOS to control the router. Cisco technology is in the IOS, not in the hardware.

### 2.1.5 Operation of Cisco IOS software

There are numerous IOS images for different Cisco device models. Each device uses a similar basic command structure for configuration. The configuration and troubleshooting skills acquired on a specific device will apply to a variety of products.

The naming convention for the different Cisco IOS Releases contains three parts:

- The platform on which the image runs
- The special capabilities and feature sets supported in the image
- Where the image runs and whether it has been zipped or compressed

One of the major constraints for the use of a new IOS image is compatibility with the router flash and RAM memory.

The students should also understand that the same IOS is used on the smallest to the largest Cisco products. This will assure students that the skills they develop on small Cisco routers can be applied to larger routers and switches.

Show students various naming conventions and identify the three parts of the naming convention. For example, in `cpa25-cg-1`, `cpa25` is the Cisco Pro 2500 Router, `cg` is the feature capability such as communication server, remote-access server, or ISDN, and the `1` is the run location or compressed status.

Explain that it is important to install and maintain various IOS versions, especially newer versions with advanced features. Encourage the students to conduct research online at [www.cisco.com](http://www.cisco.com) for more information on how to obtain various IOS images.

## 2.2 Starting a Router

**Essential Labs:** 2.2.1, 2.2.4, and 2.2.9

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can describe the purpose and fundamental operation of the router IOS

**Certification-Level Claim:** Students can establish communication between a terminal device and the router IOS and use it for system analysis, configuration, and repair

**Hands-on skills:** none

### 2.2.1 Initial startup of Cisco routers

This section teaches students about the startup process for a router. Students learn how to establish a HyperTerminal session and log into a router. Students will then be introduced to the help feature and enhanced editing commands.

When a Cisco router powers up, it performs a POST. This executes diagnostics from ROM on all hardware modules. After the POST, the following events occur as the router initializes:

- Bootstrap is loaded from ROM.
- IOS is loaded from flash, TFTP, or ROM.
- Config is loaded from NVRAM or TFTP into setup mode.

This section teaches students how to check the configuration during the boot process. Setup mode is intended to quickly install a router with minimal configuration. Discuss the initial startup of routers and explain why the IOS and configuration files can be loaded from several places.

### 2.2.2 Router LED indicators

Router LED indicators indicate the status of a router. If an interface is extremely busy, its LED will be on all the time. The green LED will be on after the router card initializes correctly.

Have the students view the LED indicators on the routers in the lab setup. Show them LEDs that work correctly and explain what they are. Make sure the students understand that the port status and link LEDs are the prime indicators of the physical layer status.

### 2.2.3 The initial router bootup

Bootup messages displayed by a router include messages such as “NVRAM invalid, possibly due to write erase”, which indicates that the router has not been configured or the backup configuration has been erased.

If a router does not boot up correctly, issue the **show version** command to examine the configuration register to see if it is booting.

Remind the students that the router is a special purpose computer. It has a boot sequence that is similar to a standard computer. The router must load the IOS from one of several sources. The router must also obtain a configuration file. If a configuration file is not available, the router will enter setup mode, which prompts the user for a basic router configuration. Make sure the students understand what the router needs as basic configuration information. This provides a lot of information about how the router works. It is very important for students to understand the difference between the IOS and the configuration file.

## 2.2.4 Establish a console session

To establish a HyperTerminal Console session, students should complete the following steps:

1. Connect the terminal with an RJ-45-to-RJ-45 rollover cable and an RJ-45-to-DB-9 or RJ-45-to-DB-25 adapter
2. Configure the terminal or PC terminal emulation software for 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control

Instruct the students to connect the cables from the router to the PC and to connect with the HyperTerminal program. To configure a router, a connection must be established between the PC and a router. Make sure students understand that this is how routers need to be configured initially, but it is not the only way to configure a router.

## 2.2.5 Router login

There are two levels of access to commands in a router:

- User EXEC mode
- Privileged EXEC mode

The user EXEC mode is a view-only mode. Enter privileged EXEC mode with the **enable** command from the User prompt. Other modes can be accessed from privileged mode to configure a router. The students should have a lot of practice with hands-on activities in the lab setup. It is important for students to understand the various modes to be able to accurately configure a router. It is not necessary to memorize all commands. Students must understand each mode so they can make the configurations from the correct locations.

## 2.2.6 Keyboard help in the router CLI

At the user mode prompt, a question mark (?) should be typed to display a list of commands available in the router. From user mode, the **enable** command will switch the router into the privileged mode. If a question mark (?) is entered from the privileged mode prompt, many more commands are listed as available commands to use in the router. Students should briefly review the types of commands in each mode. There is no need to memorize all of the commands.

The context-sensitive help is one of the most useful features of the IOS. Teach the student that the question mark (?) is extremely helpful in the router.

To demonstrate the help feature, instruct students to set the clock without telling them which commands to use. The question mark (?) will guide students through the process.

### 2.2.7 Enhanced editing commands

Enhanced editing commands are on by default. To disable enhanced editing mode, the `terminal no editing` command can be used at the privileged mode prompt.

The `editing` command set provides a horizontal scrolling feature for commands that extend beyond a single line. When the cursor reaches the right margin, the command line shifts ten spaces to the left. The first ten characters of the line cannot be seen, but a user can scroll back to check the syntax. It is represented by a dollar sign (\$).

Some of the editing commands are as follows:

- **Ctrl-A** moves to the beginning of the command line.
- **Ctrl-B** moves back one character.
- **Ctrl-E** moves to the end of the command line.
- **Ctrl-F** moves forward one character.
- **Ctrl-Z** moves back out of configuration mode.
- **Esc** and then **B** moves back one word.
- **Esc** and then **F** moves forward one word.

The syntax of IOS commands can be complex. Keyboard editing features can be used to correct text that has been entered. When a router is being configured, repetitive command statements, typing errors that need to be fixed, and commands that need to be reused may be encountered. Questions about the **Ctrl** key and **Esc** key sequences will probably appear on the CCNA exam.

### 2.2.8 Router command history

The user interface provides a history of commands that have been entered. This feature can be used to recall long or complex commands. The command history feature can be used to complete the following tasks:

- Set the command history buffer size
- Recall commands
- Disable the command history feature

By default, the command history records ten command lines in the history buffer. To recall commands, press **Ctrl-P** or the **Up Arrow** key to recall repeated commands. Press **Ctrl-N** or the **Down Arrow** key to recall more recent commands in the history. The **Ctrl-P** and **Ctrl-N** features are also likely to be tested on the CCNA exam.



The syntax of IOS commands can be complex. The feature used to recall commands can help students save time when they program or troubleshoot a router.

### 2.2.9 Troubleshooting command line errors

This troubleshooting lab allows students to log into the router and access various modes. Demonstrate the use of the question mark (?) as a helpful tool for students who do not know which command to enter.

Also demonstrate the use of the **history** command as a helpful tool for students to troubleshoot problems without retyping repeated commands.

### 2.2.10 The **show version** command

The **show version** command displays information about the Cisco IOS software version. This information includes the system image file name and the location from which it was booted. It also contains the configuration register and the boot-field setting. Explain that an important aspect of router and IOS maintenance is to know exactly which version of the IOS is being used.

Cisco has numerous major and minor IOS releases. There are many different versions and different features to meet the requirements of a network. Students should know that the **show version** command shows much more than just the version of the IOS. This is an important command. Explain to students that this is the only command that can be used to examine the configuration register.

## Module 2 Summary

Before students move on to Module 3, they must be able to interact with the router through a HyperTerminal session and the CLI.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 2 exam. Make sure students know how to access the command-line prompt. Formative assessments related to lab work are relevant to Module 2.

Students should understand the following main points:

- Understand the basic operation of IOS
- Identify various IOS features
- Identify methods to establish a CLI session with the router
- Use HyperTerminal to establish a CLI session
- Log into the router
- Use the help feature in the command line interface
- Use the enhanced editing commands
- Use the command history
- Troubleshoot command line errors
- Use the **show version** command

# Module 3: Configuring a Router

## Overview

When teaching Module 3, emphasize the empowerment that students will gain from the ability to configure routers and the importance of familiarity with the IOS through extensive practice. There are many tools available to teach IOS:

- The curriculum text and graphics are used to introduce command syntax and context.
- The online command references are integrated.
- CiscoPedia is the IOS command reference in the form of a Windows help file. All CCNA and CCNP commands are included.
- Integrated e-Labs provide guided practice of command syntax.
- Standalone e-SIMs provide more open-ended practice of CCNA 2-level router configuration.
- Hands-on labs are integrated PDF files that should be the core of the learning experience.

### Module 3 Caution

Spend a lot of time on this module. Students have wanted to program routers since the first day of CCNA 1. This module presents the core skills that the students will use to build all Cisco device configurations. From this point in the CCNA 2 curriculum through the end of the CCNA 4 curriculum, students may be deprived of the opportunity to learn about the IOS if the student-to-equipment ratio is high. Only the local instructor can decide what mix of lab equipment, group work, creative rotations, lab access, remote access through NetLabs or other solutions, e-Labs, e-SIM, CiscoPedia, and other tools can be used to give students adequate opportunities to learn IOS.

After completing this module, students should be able to perform the following tasks:

- Name a router
- Set passwords
- Examine `show` commands
- Configure a serial interface
- Configure an Ethernet interface
- Make changes to a router
- Save changes to a router

- Configure an interface description
- Configure a message-of-the-day banner
- Configure host tables
- Understand the importance of backups and documentation

## 3.1 Configure a Router

**Essential Labs:** 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, and 3.1.7

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can perform, save, and test an initial configuration on a router.

**Certification Level Claim:** Students can perform an initial configuration on a router.

**Hands-on skills:** none

### 3.1.1 CLI command modes

The students need to understand that the router does not know what routing to do until it is configured. This section will help students begin the configuration of a router.

To gain access to a router, a login is required. After login, there is a choice of modes. The modes interpret the commands that are typed and perform the operations. There are two EXEC modes:

- User EXEC mode
- Privileged EXEC mode

The first configuration mode is referred to as global configuration mode or global config. The following configuration modes are available in global configuration mode:

- Interface
- Subinterface
- Controller
- Map-list
- Map-class
- Line
- Router

Global configuration commands are used in a router to apply configuration statements that affect the entire system. Use the privileged EXEC command **configure terminal** to enter global configuration mode.

Explain that Cisco IOS is modal. Emphasize that in the CLI that there are different modes to accomplish different tasks. There are several advantages to this. One is that the commands are generally shorter because the object of the mode, i.e., the interface, or routing protocol, to

be changed does not need to be specified in the command. Another advantage is that only the parameters, or objects of the mode, i.e., the interface, or routing protocol, can be modified by the command. This helps prevent accidental configuration of the wrong object. There are shortcuts to show students at a later time:

- `config t` for `configure terminal`
- `int fa0/0` for `interface fastethernet 0/0`

Students commonly enter the correct command at the incorrect prompt. If the students are unable to enter a command, check the mode. The prompt will be either `Router(config)#` or `Router(config-if)#`.

Ask students the following questions:

- Which mode is the user in when first logging into the router?
- What mode is the user in after entering the `enable` command?

### 3.1.2 Configuring a router name

One of the first basic configuration tasks is to name a router. This task helps with network management and uniquely identifies each router within a network. Use global configuration mode to name a router. The name of a router is called the hostname and will be displayed as the system prompt. If a router is not named, then the system default will be “Router”.

Students need to understand that the name is an important part of the configuration process. Much of the configuration and troubleshooting will be performed remotely. Users will telnet into different routers. For practice, ask students to name the routers. When instructors are asked to help troubleshoot a lab, they can easily identify the different routers. The router name at the prompt confirms the student has completed this task. Students should also understand that names should be chosen to represent a location or a function. In many organizations, there are naming conventions to be followed.

Ask students the following questions:

- What is the default name of the router?
- In which mode can the user name the router?
- What is the command to name a router?

### 3.1.3 Configuring router passwords

Passwords can be used to secure a router and restrict access. Passwords can be established for virtual terminal lines and the console line. The privileged EXEC mode may also have a password. From global configuration mode use the `enable password` command to restrict access to the privileged mode. The line configuration mode can be used to establish a login password on the console terminal. Use the command `line vty 0 4` to establish a login password on incoming Telnet sessions.

Discuss the differences between the various passwords. Students need to understand when each password is used. If students ask if user ids and passwords can be used instead of just passwords, the answer is that they can, but that is beyond the scope of this course.

Ask students the following questions:

- What is the command to set the enable password?
- What is the command to set the telnet password?
- What is the command to set the console password?

### 3.1.4 Examining the show commands

There are many **show** commands, which are used to examine the contents of files in the router and for troubleshooting. From each mode in the router, the **show ?** command can be used to see all the available options. Some of the **show** command options are as follows:

- show interfaces
- show controllers serial
- show clock
- show hosts
- show users
- show history
- show flash
- show version
- show ARP
- show protocol
- show startup-configuration
- show running-configuration

Students may want to use the **show running-config** command as their primary troubleshooting tool. This is not a good habit. It is probably the quickest way to find problems in the simple configurations used in this course. However, that is not true in most situations. Students should learn to use the **show running-config** command to confirm suspected problems. Some CLI shortcuts to show students in the future are as follows:

- **sh int fa0/0** for show interface fastethernet 0/0
- **sh run** for show running-configuration
- **sh run int fa0/0** for show running-configuration fastethernet 0/0

Ask students the following questions:

- Which command will show the configuration file in NVRAM?
- Which command will show the configuration file in RAM?

### 3.1.5 Configuring a serial interface

A serial interface can be configured from the console or through a virtual terminal line. By default, Cisco routers are DTE devices but they can be configured as DCE devices. To configure a serial interface follow these steps:

1. Enter global configuration mode.
2. Enter interface mode.
3. Specify the interface address and subnet mask.
4. Set the DCE clock rate. Skip this step on DTE.
5. Turn on the interface.

There are two important items in this TI.

The first item is that setting a clock rate is not a normal configuration item. It is only done to simulate a WAN. The clock is normally provided by the DCE equipment such as a CSU. The curriculum shows the command entered as `clock rate`, but on some Cisco routers the command can be entered as `clockrate`. Both will result in the same running configuration.

The second item is that interfaces are shutdown by default and must be enabled with the `no shutdown` command. The `shutdown` command will turn off an interface. Instruct students to check for interfaces that are shutdown when troubleshooting the student labs. This can be checked by typing `show interface serial 0/0` or `show run int serial 0/0` for the interface serial 0/0.

Ask students the following questions:

- What command turns on an interface?
- What command turns off an interface?
- What command is entered on an interface at the DCE end of the cable?

### 3.1.6 Making configuration changes

To verify changes, use the `show running-config` command. This command will display the current configuration. If the intended variables are not displayed, the environment can be corrected in the following ways:

- Issue the `no` form of a configuration command.
- Restart the system and reload the original configuration file from NVRAM.



- Remove the startup configuration file with the **erase startup-config** command.
- Restart the router and enter setup mode.

To save the configuration variables to the startup configuration file in NVRAM, enter the following command at the privileged EXEC prompt:

```
Router#copy running-config startup-config
```

Students must understand that any changes that are made to the configuration will occur immediately. These changes are made to the running configuration. Students must also realize that configuration changes need to be saved to the startup configuration. If they are not, then they will be lost when the router is restarted. Students should shut down interfaces during configuration and enable the interface after the configuration changes are completed.

Ask students the following questions:

- Which command will erase the configuration file in NVRAM?
- Which command will erase the configuration file in RAM?
- Which command will copy the RAM to NVRAM?
- Which command will copy the NRAM to RAM?

### 3.1.7 Configuring an Ethernet interface

An Ethernet interface can be configured from the console or a virtual terminal line. By default, interfaces are disabled. Use the **no shutdown** command to enable an interface. Use the **shutdown** command to turn off an interface if it needs to be disabled for maintenance or troubleshooting. The following command is used to configure interface serial 0/0. The interface will change to up. Both ends of the serial cable need to be configured for the interface to stay in an up state:

```
rt1(config)#interface serial 0/0

rt1(config-if)#ip address 192.168.0.1 255.255.255.0

rt1(config-if)#no shutdown

00:20:46: %LINK-3-UPDOWN: Interface Serial0/0, changed state to
up

00:20:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up

rt1(config-if)#
```

## 3.2 Finishing the Configuration

**Essential Labs:** 3.2.3, 3.2.5, 3.2.7, and 3.2.9

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can configure additional administrative functionality on a router

**Certification-Level Claim:** Students can configure a router for additional administrative functionality.

**Hands-on skills:** none

### 3.2.1 Importance of configuration standards

This section introduces the importance of configuration standards. The following topics are covered:

- Configuration of interface descriptions
- Message-of-the day banners
- Configuration of host tables
- Backup configuration documentation

In many organizations, standards are either treated very seriously or there are no standards. It is important to develop standards for configuration files within an organization. These can be used to control the number of configuration files that must be maintained, how the files are stored, and where the files are stored.

In organizations where standards are treated seriously, students need to understand that it is very important for the standards to be followed. In organizations where there are no standards, students can introduce standards to add value to the organization.

Students need to understand why standards are important and begin to apply them in the lab. Encourage students to create and use standards. Remember to simulate real-world environments in the classroom and lab.

A centralized support standard is necessary to manage a network. Configuration, security, performance, and other issues must be adequately addressed for the network to function properly. The creation of standards for network consistency helps reduce network complexity, the amount of unplanned downtime, and exposure to network impacting events. Emphasize that there should be a standard for everything and that each standard should be a written part of the documentation and procedures. These should include how configuration files are named, how interfaces are addressed, and the description used on interfaces.

The use of these standards is very important for troubleshooting. Explain to students that the same network associate will not always troubleshoot the network device. If the previous

associate did not have or follow standards, then the next associate will need to analyze how the device is supposed to be connected or configured. For example, if the headquarters router always has the lowest address in a subnet configured and the remote office uses the next address up, then there is no question about what the interface addresses should be. The interface description should provide information about the configuration, connection, and use of the interface.

### 3.2.2 Interface descriptions

The description of an interface should be used to identify important information such as a distant router, a circuit number, or a specific network segment. A description of an interface can help a network user remember specific information about the interface such as which network the interface services.

The description is a comment about the interface. Stress the importance of a standard type of description. Students will use small routers in a small topology and can get physical access to the routers. Since this is the extent of their experience, it is hard for them to understand how helpful interface descriptions are.

Ask the students to envision an environment with hundreds of routers, thousands of interfaces, and routers that are 1000 kilometers (621.4 miles) away. Tell the students that a customer from a branch office is unable to connect to headquarters. Ask students how they can verify that the interface is connected to the correct branch office before they change anything on the interface. There are several good answers such as ask the customer, refer to documentation, and use the `show cdp neighbor` command. The best answer is to look at the interface description with the `show interface` command.

Ask students the following questions:

- What is used on an interface to make a comment?
- Which type of information may be included in a description?

### 3.2.3 Configuring an interface description

To configure an interface description, enter global configuration mode. From global configuration mode, enter interface mode. Use the following steps:

1. Enter global configuration mode with the `configure terminal` command.
2. Enter a specific interface mode such as `interface ethernet 0`.
3. Enter the `description` command followed by the information to be displayed. For example, XYZ network, Building 10.
4. Exit interface mode and return to global configuration mode by pressing **Ctrl-Z**.

Save the configuration changes to NVRAM with the `copy running-config startup-config` command.

Important concepts for students to understand are that each description is for a particular interface and the description is entered in interface configuration.

Ask students the following questions:

- Which configuration mode is used to enter the description?
- What are the commands to add a description to an interface?

### 3.2.4 Login banners

Students must realize that a login banner can be seen by anyone.

This login banner should be a warning that users should not attempt to log in unless they are authorized. A message such as “This is a secure system, authorized access only!” instructs unwanted intruders to beware. A login banner is a message that is displayed at login and can be used to convey messages that affect all network users such as system shutdowns. Make sure students understand that these banners should be warnings and not invitations.

Ask students the following questions:

- Who can see a login banner?
- What is an example of a good login banner?
- Where is the login banner displayed?

### 3.2.5 Configuring message-of-the-day (MOTD)

A message-of-the-day (MOTD) banner can be displayed on all connected terminals. Students must enter global configuration mode to configure a message-of-the-day banner. They should use the `banner motd` command, followed by a space and a delimiting character such as the pound sign (#). Next, students should add a message of the day followed by a space and the delimiting character again. Instruct students to follow these steps to display a message-of-the-day:

1. Enter global configuration mode with the `configure terminal` command.
2. Enter the `banner motd # message of the day #` command.
3. Save changes with the `copy running-config startup-config` or `copy run start` command.

### 3.2.6 Host name resolutions

Protocols such as Telnet use host names to identify network devices or hosts. Network devices such as routers must be able to associate host names with IP addresses to communicate with other IP devices.

Each unique IP address can have a host name associated with it. The Cisco IOS software maintains a cache of host name-to-address mappings for use by EXEC commands. A host name resolution is the process a computer system uses to associate a name with a network address.

Ask students the following questions:

- What is a host name is associated with?
- Can each unique IP address have a host name associated with it?

### 3.2.7 Configuring host tables

This is a simple process. Students need to understand that the host table provides local host resolution.

### 3.2.8 Configuration backup and documentation

The configuration of network devices determines the behavior of a network. The following tasks are used to manage device configurations:

- List and compare configuration files on devices
- Store configuration files on network servers
- Perform software installations and upgrades

Configuration files should be stored as backup files. Configuration files can be stored on a network server, on a TFTP server, or on a disk that is stored in a safe place. Configuration backup files and documentation should be stored in a safe place in case there is a need to recover these files later.

For example, the startup-configuration of a router can be stored in another place such as on a network server or on a TFTP server as a backup. If the router goes down, the stored file could be placed back on the router. This would minimize the down time.

Configuration management is an important aspect of network management. The backups of the configurations should be current and maintained in multiple locations. These backups should be available for maintenance and troubleshooting, but protected from unauthorized access. Configurations can be used by hackers to gain useful information about a network infrastructure.

Ask students the following questions:

- What is the purpose of configuration backup and documentation?
- Where can the configuration files be stored?
- What would minimize the down time of a router?

### 3.2.9 Backing up configuration files

A current copy of the configuration can be stored on a TFTP server. The **copy running-config tftp** command can be used to store the current configuration on a network TFTP server. A router can be configured by loading the configuration file stored on one of the network servers. The configuration of a router can also be saved to a disk or hard drive by

capturing text in the router. If the file needs to be copied back to the router, it can be pasted into the router.

Ask students the following questions:

- What is the command used to copy RAM to NVRAM?
- What is the command used to copy NVRAM to RAM?

## Module 3 Summary

Before students begin Module 4, they must be able to perform a basic router configuration in a limited amount of time and without assistance. Basic configuration includes hostnames, passwords, interfaces, and the ability to verify their work with `show` commands.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 3 exam. Formative assessments can also be conducted as students work on the routers to monitor how well a lab is performed.

This section summarized the main points in router configuration. The router has several modes:

- User EXEC mode
- Privileged EXEC mode
- Global configuration mode
- Other configuration modes

The CLI can be used to make changes to the configuration such as the following:

- Set the hostname
- Set passwords
- Configure interfaces
- Modify configurations
- Show configurations

Students should understand the following main points:

- Configuration standards are important elements in the ability of any organization to maintain an efficient network.
- Interface descriptions can include important information to help network administrators understand and troubleshoot their networks.
- Login banners and messages-of-the-day provide users with information when they log in to the router.
- Host name resolutions translate names to IP addresses to allow the router to quickly convert names to addresses.
- Configuration backup and documentation is extremely important to keep a network operating properly.

# Module 4: Learning about Other Devices

## Overview

Module 4 will introduce students to the Cisco Discovery Protocol (CDP). CDP is enabled by default on all Cisco devices. CDP allows devices such as Cisco routers to obtain information about directly connected routers, switches, and bridges. CDP functions at Layer 2 in the OSI model. It operates independently of Layer 3, which means that devices can gather information about other directly connected devices regardless of network layer protocol issues.

The first lesson will explain how CDP is used to acquire information about neighboring routers. Students should already know how to use serial and Ethernet connections to physically connect routers. Students should also know how to use programs such as HyperTerminal and Telnet to perform router configuration tasks. Review these skills if necessary. Have students perform a standard lab-setup configuration as an optional skill review.

The second lesson will introduce students to the TCP/IP protocol Telnet. Telnet is a remote connection utility that allows network administrators to perform configuration and management tasks on routers and switches. Students will learn how to establish, manage, and terminate Telnet sessions with remote devices. Students should already be familiar with basic router setup and configuration. Students should possess basic router configuration skills and be able to physically connect the devices. Students will use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console.

### Module 4 Caution

Most students do not understand that CDP and Telnet are powerful troubleshooting tools. At this point, it is important to provide additional support for students who have not mastered Module 3. Cover this module extensively. Many of the next modules are lab intensive and time intensive.

Students who complete this module should be able to perform the following tasks:

- Enable and disable CDP
- Use the `show cdp neighbors` command
- Determine which neighboring devices are connected to which local interfaces
- Use CDP to gather network address information about neighboring devices
- Establish a Telnet connection
- Verify a Telnet connection
- Disconnect from a Telnet session
- Suspend a Telnet session
- Perform alternative connectivity tests



- Troubleshoot remote terminal connections

## 4.1 Discovering and Connecting to Neighbors

**Essential Labs:** 4.1.4 and 4.1.6

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can use embedded data-link layer functionality to perform network neighbor discovery and analysis from the router console.

**Hands-on skills:** none

### 4.1.1 Introduction to CDP

CDP is a Cisco proprietary protocol that is used for Layer 2 troubleshooting and network documentation. CDP is used to acquire protocol and platform information from neighboring devices. It is enabled by default on Cisco devices and requires all media that is used to be Subnetwork Address Protocol (SNAP) enabled. Most media is SNAP enabled.

During the boot-up process, each Cisco device sends CDP advertisements to a multicast address to collect information from its neighbors. These advertisements are periodically repeated so that updated information can be gathered. CDP advertisements are also used by the receiving devices to learn about the sender. CDP information is dynamic. It is constantly updated through periodic advertisements. Reporting devices provide a Time-to-Live (TTL) value for the data.

CDP operates at Layer 2 and is upper layer independent. Review Figure 1 with students. CDP allows each Cisco device to collect information from its neighbors regardless of the Layer 3 protocols the devices are configured to use. Discuss the following characteristics of CDP:

- CDP runs on all Cisco devices such as routers, switches, and bridges.
- CDP is Cisco proprietary.
- CDP is upper-layer independent.
- CDP information is exchanged only by directly-connected neighbors.

Students may not be familiar with multicasting. A brief explanation may be required at this point. The following link provides information on Cisco IP multicast implementation.

<http://www.cisco.com/warp/public/732/Tech/multicast>

## 4.1.2 Information obtained with CDP

CDP is used to collect information about directly-connected devices. The types of information it collects are referred to as Type Length Values (TLVs). This TI includes a table that defines each TLV. Certain types of information are only included as a part of CDPv2. This information is noted in the table.

TLV	Definition
Device-ID TLV	Identifies the device name in the form of a character string
Address TLV	Contains a list of network address of both receiving and transmitting devices
Port-ID TLV	Identifies the port on which the CDP packet is sent
Capabilities TLV	Describes the functional capabilities of a device in the form of a device type such as a switch
Version TLV	Contains information about the software release version on which the device is running
Platform TLV	Describes the hardware platform name of the device
IP Network Prefix TLV CDPv2	Contains a list of network prefixes to which the sending device can forward IP packets. This information is in the form of the interface protocol and port number such as Eth 0/1
VTP Management Domain TLV CDPv2	Advertises the configured VTP management domain name string of a network and is used by network operators to verify VTP domain configuration in adjacent network nodes
Native VLAN TLV CDPv2	Indicates the assumed VLAN for untagged packets on each interface and is implemented only for interfaces that support the IEEE 802.1Q protocol
Full or Half Duplex TLV	Indicates the status duplex configuration of a CDP broadcast interface and is used by network administrators to diagnose connectivity problems between adjacent network devices

The `show cdp neighbors` command displays CDP information collected by a device about its neighbors. It can be issued at a console connected to a Cisco network device.

Demonstrate the `show cdp neighbors` command and the `show cdp neighbors detail` command. Note that much of the information outlined in the table can only be seen if the `detail` option is utilized. This command variation is seen in subsequent RIOs. Some information is only displayed with CDPv2, which is implemented with IOS version 12.0(3)T.

Demonstrate how the `show cdp neighbors` command and its variations can be consoled into a router that is connected to another router or a switch to show students the output.

The `show cdp neighbors` command allows students to perform the associated Flash e-Lab.

### 4.1.3 Implementation, monitoring, and maintenance of CDP

CDP implemented by default on all interfaces that support it. The following table lists variations of the CDP command and their functions. These commands should be used in privileged EXEC mode. The table is located in this section of the curriculum.

Although not noted in the curriculum, many of these commands can be executed in user mode. Some of the configuration commands are done in global configuration mode and some require interface configuration mode.

Discuss the `cdp enable` and `cdp run` commands. The `cdp enable` command is an interface configuration command that enables CDP on a particular interface. The `cdp run` command is a global configuration command that enables CDP on a Cisco device. Students should also be comfortable with the `no` form of these commands. Relevant TIs from CCNA 2 v2.1.4 are 4.3.3 and 4.3.4.

Demonstrate command usage after the class reviews the table.

Command	Purpose
<code>cdp enable</code>	Enables CDP on an interface
<code>cdp advertise-v2</code>	Enables CDP Version-2 on an interface
<code>clear cdp counters</code>	Resets the traffic counters to zero
<code>show cdp</code>	Displays the interval between transmissions of CDP advertisements, the number of seconds the CDP advertisement is valid for a given port, and the version of the advertisement
<code>show cdp entry entry-name [protocol   version]</code>	Displays information about a specific neighbor, which can be limited to protocol or version information
<code>show cdp interface [type number]</code>	Displays information about interfaces on which CDP is enabled
<code>show cdp neighbors [type number] [detail]</code>	Displays the type of device that has been discovered, the name of the device, the number and type of the local interface or port, the number of seconds the CDP advertisement is valid for the port, the device type, the device product number, and the port ID Displays information on the native Vlan ID, the duplex mode, and the VTP domain name associated with neighbor devices when the <code>detail</code> keyword is used

### 4.1.4 Creating a network map of the environment

CDP uses advertisements to collect information about its neighbors. Its limitation is that it only collects information from directly-connected devices. The `telnet` command can be used in conjunction with `cdp` commands to create a network map. To do this, a network administrator can console into one router and use the `telnet` command to move from router to router.

If students have limited or no experience with the use of Telnet to move from device to device, this concept and skill should be reviewed. If students do not understand this capability, it will be difficult to understand the procedure described in this RIO. Demonstrate this capability if necessary. Refer to the figure to show students how `telnet` is used to map a network. Allow students to practice use of this command. Instruct students to map their router setup or a setup performed by another group.

#### 4.1.5 Disabling CDP

Although CDP is enabled by default on all Cisco devices there may be situations in which CDP must be disabled. Three examples are included in the TI:

- If the bandwidth of a particular connection is inadequate, CDP can be disabled to conserve bandwidth.
- Since CDP is a Cisco proprietary device, if there is only one Cisco device on a network segment then there is no device with which to share information.
- If a particular device is connected to some other network such as an ISP, CDP can be disabled for security reasons. This will prevent the device from advertising information about itself to outside devices.

CDP can be disabled at two levels:

- The `no cdp run` command can be used in global configuration mode to disable CDP for the entire device. This should be used when only one Cisco device is present and CDP would serve no purpose on the network segment.
- CDP can be disabled for a specific interface. The network administrator must be in interface mode to perform this task. The command is `no cdp enable` or `no cdp advertise-v2`, based on the version of CDP that is used.

To determine if a particular interface has CDP enabled, the `show cdp interface` command can be used in user or privileged mode. The figures show the use of these commands.

Make sure students realize that CDP is enabled on all interfaces by default. Demonstrate how to disable CDP at the interface level and globally. Allow students to perform these commands on their own lab setup but ensure that students enable CDP when they are finished.

#### 4.1.6 Troubleshooting CDP

CDP does not require any configuration. However there may be times when some of the following commands may be helpful in the troubleshooting process. A common problem may be devices with different versions of CDP. The `show cdp neighbor` command will show whether or not a device exists in the CDP neighbor cache and indicate if a device is utilizing version 2 of CDP.

<b>Command</b>	<b>Purpose</b>
<code>clear cdp table</code>	Deletes information about neighbors from the CDP table
<code>clear cdp counters</code>	Reset traffic counters to zero
<code>show cdp traffic</code>	Displays CD counters such as the number of packets sent and received and checksum errors
<code>show debugging</code>	Displays information about the types of debugging that are enabled for the router
<code>debug cdp adjacency</code>	Displays CDP neighbor information
<code>debug cdp events</code>	Displays CDP events
<code>debug cdp ip</code>	Displays CDP IP information
<code>debug cdp packets</code>	Displays CDP packet-related information
<code>cdp timers</code>	Specifies how often the Cisco IOS software sends CDP updates
<code>cdp holdtime</code>	Specifies the hold time to be sent in the CDP update packet
<code>show cdp</code>	Displays global CDP information such as timer and hold-time information

Review the following key points:

- CDP is Cisco proprietary.
- CDP runs on any SNAP-enabled media.
- CDP functions at Layer 2 and functions independent of the upper layers.
- CDP is used by all Cisco network devices such as routers, switches, and bridges.
- CDP utilizes periodic advertisements to obtain or update information about directly-connected devices

Have students perform the CDP neighbor lab.

### **Web Links**

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun\\_r/frprt3/frd3001b.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3001b.htm)

## 4.2 Getting Information about Remote Devices

**Essential Labs:** 4.2.2, 4.2.3, 4.2.4, 4.2.5a, 4.2.5b, and 4.2.6

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can perform simple LAN troubleshooting.

**Certification-Level Claim:** Students can troubleshoot a device that is part of a working network.

**Hands-on skills:** none

### 4.2.1 Telnet

Telnet provides network administrators with remote connection capability. It is a part of the TCP/IP protocol suite that operates at the application layer of the OSI model and the application layer of the TCP/IP model. The Telnet service in Cisco devices operates as a virtual terminal utility. Administrators can use Telnet to issue IOS commands when they are not directly connected to the device. Telnet consumes a vty session on the router when it is used. Remind students that vty lines 0 through 4 can be configured in a router configuration. Since Telnet is a vty connection, a router will support simultaneous Telnet connections.

Telnet also provides a tool for troubleshooting. The establishment of a Telnet connection confirms the connectivity and functionality of the application layer. The **ping** command only confirms Layer 3 connectivity.

### 4.2.2 Establishing and verifying a Telnet connection

From the router console, Telnet can be used to connect to remote devices. The administrator must type in the name of a router or the IP address of an interface to establish a Telnet connection. The following commands can be used:

```
Router>131.108.100.152
Router>paris
Router>connect paris
Router>telnet paris
```

The figure includes an explanation of Telnet. The example shows how to console into a directly connected router and then establish a Telnet connection with other network devices. Telnet may also be used to connect a PC to the router, or other network device, through a network connection instead of using a direct console cable for the connection.

Students may not understand that Telnet is widely implemented. It is not used only within a network device to connect to other network devices. For example, Telnet can be used from the command prompt in Microsoft Windows. It can be used to connect to other PCs, servers, or devices.

Demonstrate various **telnet** connection commands.

### 4.2.3 Disconnecting and suspending Telnet sessions

Network administrators may need to establish multiple Telnet sessions. The keystroke **Ctrl-Shift-6** and then the letter **X** can be used to suspend a current Telnet session. The suspend feature can be used to establish an additional Telnet session to another device. The **show sessions** command displays a numbered list of current Telnet sessions like the following example.

```
Conn Host          Address          Byte Idle Conn Name
   1 lab-a         192.168.10.1    0   0 lab-a
*  2 lab-e         192.168.10.1    0   0 lab-e
```

A connection can be resumed by selecting the corresponding number.

The **disconnect** command will terminate a specific Telnet session.

The procedure for disconnecting a Telnet session is as follows:

- Enter the **disconnect** command.
- Follow the command with the name or IP address of the router.
- Example: Denver> **disconnect paris**

The procedure for suspending a Telnet session is as follows:

- Press **Ctrl-Shift-6** and then the letter **X**.
- Enter the name of the router or IP address of the next connection.

Students often think that the **Ctrl-Shift-6**, then **X** sequence will terminate a Telnet session. They need to understand that this only suspends the session. They also need to know how to resume and terminate a session

### 4.2.4 Advanced Telnet operation

A user may have multiple Telnet sessions open at the same time. The number is limited by the session limit. The user can switch between these sessions with the **Ctrl-Shift-6** and then **X** key sequence. To resume a Telnet session, the **resume** command with the session id may be used. The connection id of all open Telnet sessions can be viewed with the **show sessions** command.

Command	Purpose
<b>Ctrl-Shift-6</b> then <b>X</b>	Escapes the current connection and returns to the EXEC prompt
<b>resume</b>	Makes the connection

The **resume [session number]** command can be used to resume a Telnet session. The process id of a session can also be entered to resume the session.

The **show sessions** command output is as follows:

```
Stanly_Lab#show sessions
Conn Host          Address           Byte Idle Conn Name
  1 lab-b          192.168.10.1      4   5 lab-b
  2 lab-d          192.168.10.1      0   0 lab-d
* 3 lab-e          192.168.10.1      0   0 lab-e
```

#### 4.2.5 Alternative connectivity tests

Connectivity can be tested with several other commands such as **ping**, **traceroute**, and **show ip route**. The **ping** command uses ICMP to send an echo request to a destination and then awaits an echo reply from that destination. This is a good test for basic connectivity, reliability, and delay. This test can be performed from the user or privileged EXEC mode. A successful ping is indicated by exclamation points (!). A period (.) indicates a ping that has timed out.

The **traceroute** command is used to view the path that packets use to reach a particular destination. This is an excellent test to identify where packets are dropped in the network. An asterisk (\*) indicates that the probe timed out. Traceroute will continue to reach the next router in a path until the process times out or it is interrupted by the **Ctrl-Shift-6** escape sequence.

The purpose behind the **traceroute** command is to record the source of each ICMP "time exceeded" message to provide a trace of the path the packet took to reach the destination. The device executing the **traceroute** command sends out a sequence of User Datagram Protocol (UDP) datagrams, each with incrementing Time-To-Live (TTL) values, to an invalid port address (Default 33434) at the remote host.

First, three datagrams are sent, each with a TTL field value set to 1. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first router in the path. This router then responds with an ICMP "time exceeded" message indicating that the datagram has expired. Next, three more UDP messages are sent, each with the TTL value set to 2. This causes the second router in the path to the destination to return ICMP "time exceeded" messages.

This process continues until the packets reach the destination and until the system originating the **traceroute** has received ICMP "time exceeded" messages from every router in the path to the destination. Since these datagrams are trying to access an invalid port (Default 33434) at the destination host, the host responds with ICMP "port unreachable" messages indicating an unreachable port. This event signals the **traceroute** program to finish.

The **show ip route** command is used to identify the routes that are shown in the routing table. These are routes to directly connected networks, networks with static routes, or networks that have been learned through a routing protocol.

Due to many security configurations throughout the Internet, ping and trace may not always work to test connectivity through networking equipment outside of your control. Many firewalls and access-lists today do not allow ICMP traffic.



The procedure to use the **ping** command is as follows:

- **ping** *IP address* or name of destination
- Press **Enter**

The procedure to use the **trace** command is as follows:

- **trace** *IP address* or name of destination
- Press **Enter**

Demonstrate a successful ping.

```
LAB-B#ping lab-c
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echoes to 199.6.13.2, timeout is 2  
seconds: !!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max =  
32/35/36 ms
```

Demonstrate an unsuccessful ping.

```
LAB-D#ping lab-c
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echoes to 199.6.13.2, timeout is 2  
seconds: .....  
Success rate is 0 percent (0/5)
```

Demonstrate a successful trace.

```
LAB-A#trace lab-e
```

```
Type escape sequence to abort.  
Tracing the route to LAB-E (210.93.105.2)  
  
 1 LAB-B (201.100.11.2) 32 msec 24 msec 24 msec  
 2 LAB-C (199.6.13.2) 32 msec 52 msec 40 msec  
 3 LAB-D (204.204.7.2) 64 msec 64 msec 64 msec  
 4 LAB-E (210.93.105.2) 60 msec * 64 msec
```

Demonstrate an unsuccessful trace.

```
LAB-A#trace lab-d
```

```
Type escape sequence to abort.  
Tracing the route to LAB-D (204.204.7.2)  
  
 1 LAB-B (201.100.11.2) 36 msec 28 msec 24 msec  
 2 LAB-C (199.6.13.2) 36 msec 44 msec 40 msec  
 3 LAB-C (199.6.13.2) !H * !H
```

Show a routing table.

```
LAB-C#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area, E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, *
- candidate default, U - per-user static route
```

```
Gateway of last resort is not set
```

```
C 204.204.7.0/24 is directly connected, Serial0
C 223.8.151.0/24 is directly connected, Ethernet0
R 201.100.11.0/24 [120/1] via 199.6.13.1, 00:00:06, Serial1
R 219.17.100.0/24 [120/1] via 199.6.13.1, 00:00:06, Serial1
R 192.5.5.0/24 [120/2] via 199.6.13.1, 00:00:06, Serial1
C 199.6.13.0/24 is directly connected, Serial1
R 205.7.5.0/24 [120/2] via 199.6.13.1, 00:00:06, Serial1
R 210.93.105.0/24 [120/1] via 204.204.7.2, 00:00:07, Serial0
```

#### 4.2.6 Troubleshooting IP addressing issues

Addressing issues are the most common problems that occur on IP networks. Three commands can be used to perform troubleshooting:

- **telnet** – verifies the application layer software between the source and the destination. This is the most complete test mechanism available.
- **ping** – uses the ICMP protocol to verify the hardware connection and the IP address of the network layer. This is a very basic test mechanism.
- **traceroute** – is used to find failures in the path from the source to destination. Traceroute uses time-to-live values to generate messages from each router along the path.

Troubleshooting is one of the most important skills of a network associate. The majority of time in the workplace will be spent troubleshooting. Students should develop these skills at every opportunity. Help students learn the logical process, what to look for, and the tools to use. Always use the OSI model to teach troubleshooting from Layer 1 to Layer 7. For students to become proficient at troubleshooting, it must be a normal part of the labs. Each lab should include a troubleshooting session. This could be a discussion about problems that might be experienced in the lab or problems can be placed on the student network.

## Module 4 Summary

Students must master CDP and network troubleshooting commands before they move on to Module 5

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 4 exam. Students should be familiar with the equipment that is in the room with them. If they need to see how it is connected, they can look at it. Another assessment option is to put several interconnected and configured routers in a taped box with a console cable and a power strip cord coming out of it. Mark the box with the name of a distant city. Then ask the students to draw a topology map of the internetwork of that city.

Students should understand the following main points:

- How to enable and disable CDP
- How to use the **show cdp neighbors** command
- How to determine which neighboring devices are connected to which local interfaces
- How to use CDP to gather network address information about neighboring devices
- How to establish a Telnet connection
- How to verify a Telnet connection
- How to disconnect from a Telnet session
- How to suspend a Telnet session
- How to perform alternative connectivity tests
- How to troubleshoot remote terminal connections

# Module 5: Managing Cisco IOS Software

## Overview

When teaching Module 5, emphasize the importance of the router boot sequence. The router boot sequence verifies the proper operation of the router hardware, identifies the correct IOS and configuration file, and shows the location of each. This process must be understood to properly configure and operate all Cisco routers. Before students begin Module 5, they should be able to identify the purpose and operation of the IOS, use the `show version` command, and troubleshoot basic connectivity issues. In this section, students will learn about the Cisco IOS File System and how to use a variety of Cisco IOS software source options. Students will also learn how to use commands to load Cisco IOS software onto a router, maintain backup files, and upgrade Cisco IOS software.

**Module Caution:** Make sure students fully understand how to copy and paste configurations into a router. Make sure that they understand the importance of configuration management, especially backups.

Students who complete this module should be able to perform the following tasks:

- Identify the stages of the router boot sequence
- Describe how a Cisco device locates and loads the Cisco IOS
- Use the `boot system` command
- Identify the configuration register values
- Describe the files used by the Cisco IOS and their functions
- List the locations of the different file types on the router
- Describe the parts of the IOS name
- Use TFTP and copy-and-paste to save and restore configuration files
- Use TFTP to load an IOS image
- Use XModem to load an IOS image
- Use `show` commands to verify the file system

## 5.1 Router Boot Sequence and Verification

**Essential Labs:** 5.1.3 and 5.1.5

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can identify the stages of the router boot-up sequence and show how the `configuration-register` and `boot system` commands modify that sequence.

**Certification-Level Claim:** Students can describe the components of network devices.

**Hands-on skills:** none

### 5.1.1 Stages of the router power-on boot sequence

The purpose of the router boot-up sequence is to verify the operation of hardware and load the correct IOS and configuration file. The router must follow a predefined set of steps while it boots up:

- When the router is first powered-on, it executes the power-on self test (POST). These diagnostics are located in ROM and verify the proper operation of the router hardware.
- If the router passes the POST, the bootstrap loader in ROM executes. The bootstrap basically indicates a starting point in memory that will load other instructions.
- Now the router is ready to load the operating system, which is Cisco IOS. The IOS can be found in flash, TFTP, or ROM. The boot field of the configuration register will indicate the location of the IOS image.
- After the operating system is loaded and operational, the configuration file from NVRAM is loaded and executed. If no configuration file exists in NVRAM, the router will prompt the user to use a question-driven setup menu.

Review the figure in this TI with the students. This is an excellent visual representation of the different aspects of the boot process. Each student should be able to reproduce this figure from memory. Remove the configuration from NVRAM to demonstrate the process used to check for a TFTP server and then enter the setup menu. Demonstrate the use of **Ctrl-C** to exit from the setup menu.

### 5.1.2 How a Cisco device locates and loads the Cisco IOS

The router can load the Cisco IOS from several different locations that can be specified by the operator. The `boot system` commands can be used to identify a fallback sequence of locations to look for the IOS.

It is important to realize that these `boot system` commands must be saved in NVRAM to be executed at the next start-up. If no `boot system` commands are saved in NVRAM, the router will use the default fallback process, flash, TFTP, and finally ROM.

Review the figure in this section to explain the process that is followed to load the IOS. Make sure students realize that network problems can affect the process when the IOS is loaded from a TFTP server. Explain that the IOS loaded from ROM is only a subset of the IOS loaded from flash.

The figure is not complete because ROM is not included.

### 5.1.3 Using the `boot system` command

The `boot system` command can be used to specify where and the sequence in which the router will look for the IOS. After the `boot system` command has been saved to the start-up configuration in NVRAM, it will be used in the next start up to locate the IOS. When the IOS is loaded from flash memory, it is located locally, which isolates the process from any network problems that might be associated with TFTP. The IOS may be loaded from a TFTP server if the flash memory has been corrupted. If the IOS is not loaded from flash or the TFTP server, a subset of the IOS can be loaded from ROM. Make sure students understand that the IOS loaded from ROM is only a subset of the Cisco IOS software and might be an older version.

Use the `boot system` command to specify a fallback sequence and save it to NVRAM. Restart the router and allow the students to verify the boot system locations during the next start-up. Explain why it is important to save the `boot system` commands to NVRAM.

### 5.1.4 Configuration register

The configuration register is a 16-bit register that contains the boot field setting in the lowest four bits. This boot field can be changed with the `config-register` command and is verified with the `show version` command. The least significant bits indicate the location from which the router will be booted. Zero will cause the router to boot in ROM monitor mode, one will cause the router to boot from ROM, and two to F will cause the router to use the `boot system` command in NVRAM.

Configuration Register Setting	Location from which the router will boot.
0x0	ROM monitor mode, manual boot
0x1	ROM, automatic
0x2 to 0xF	NVRAM

More information can be found at the following website:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_command\\_reference\\_chapter09186a00800ca506.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca506.html)

### 5.1.5 Troubleshooting IOS boot failure

Students must be familiar with the boot sequence and the configuration register to be able to troubleshoot boot errors.

If the router does not boot properly, the **show version** command can be used to identify the configuration register setting. The boot field indicates where the router is configured to boot from and the **config-register** command is used to make any necessary changes.

If the router IOS does not boot properly, there are several things that could be wrong:

- Boot system statement in configuration file
- Incorrect configuration register value
- Corrupted flash image
- Hardware failure

Instruct students to use the **show version** command to check the configuration register value. When a router does not boot properly it is usually because the configuration register setting is incorrect. For students to understand the impact that the boot sequence and the configuration register has on routing, they must perform the hands-on labs. Make sure each student can complete and explain the labs. Discuss the results and purpose of the labs after they have been completed by all of the students.

Instruct students to verify the configuration register setting on a regular basis. Occasionally change the configuration register settings and allow them to troubleshoot the errors that occur.

### **Additional Resources**

[http://www.cisco.com/en/US/products/hw/routers/ps233/products\\_tech\\_note09186a00800a65a5.shtml](http://www.cisco.com/en/US/products/hw/routers/ps233/products_tech_note09186a00800a65a5.shtml)

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_command\\_summary\\_chapter09186a00800801b1.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summary_chapter09186a00800801b1.html)

## **5.2 Managing the Cisco File System**

**Essential Labs:** 5.2.3, 5.2.5, 5.2.6a, and 5.2.6b

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can manage system image and device configuration files.

**Certification-Level Claim:** Students can manage system image and device configuration files.

**Hands-on skills:** none

## 5.2.1 IOS file system overview

A router or switch requires software to operate. The following are two basic types of essential software:

- The operating system
- The config file

The operating system that is used in almost all Cisco devices is the Cisco IOS. The IOS is the software that allows the hardware to function as a router or a switch. The software a router or switch uses is referred to as the configuration, or config file. The configuration file contains the instructions that define how the device will route or switch.

The IOS is stored in Flash memory. The configuration file is stored in NVRAM. Discuss with the students the differences between these types of memory and help the student understand by opening a router and showing the inside of the router to the students. Discuss RAM, ROM, flash, and NVRAM. Students must understand the differences between them. One difference to discuss is that the IOS in flash or RAM is several megabytes and the configuration file in NVRAM is up to a few kilobytes.

Version 12 and newer releases of the IOS provide a single interface to all file systems. This is referred to as the Cisco IOS File System (IFS). The IFS can be used to perform all the file system management for a router. Explain that the IFS is based on UNIX file systems.

## 5.2.2 IOS naming convention

Many different versions of the IOS are available. The IOS supports many different hardware platforms and features. This is a continuous development process.

To identify the different versions, Cisco has a naming convention for the IOS files. The IOS naming convention uses different fields in the name such as hardware platform identification, feature set identification, and the numerical release.

The first part of the IOS filename identifies the hardware platform. The second part of the IOS filename identifies the various features that the file contains. The third part of the filename indicates the file format. It specifies if the IOS is stored in flash, if it is in compressed format, and if it can be released. The fourth part of the filename identifies the IOS release.

This is an important concept for students to understand. They should be able to look at an IOS filename and determine the hardware platform, features, file format, and the release. Students should also understand that these naming conventions vary for different releases. This occurs as the feature sets are rebundled and renamed.

Show students some of the tools for IOS planning that are available on the Cisco website. Most of these are only available to users who have obtained user ids through SmartNet.

<http://www.cisco.com/warp/customer/620/1.html>

[http://www.cisco.com/en/US/customer/products/sw/iosswrel/ios\\_abcs\\_ios\\_networking\\_the\\_entprise0900aecd800a4e14.html](http://www.cisco.com/en/US/customer/products/sw/iosswrel/ios_abcs_ios_networking_the_entprise0900aecd800a4e14.html)



### 5.2.3 Managing configuration files using TFTP

The active configuration uses RAM and the default location for the startup configuration is NVRAM. Students must understand the differences between RAM, ROM, NVRAM, and flash. If the configuration is lost, there should be backup copies available. The backup configuration can be stored on a TFTP server. The `copy running-config tftp` command can be used to do this.

The steps to copy to a TFTP server are as follows:

- Enter `copy running-config tftp`
- Enter the IP address of the TFTP server at the prompt
- Enter the name to assign to the configuration file
- Answer yes each time to confirm the choices

The steps to copy from a TFTP server to restore the configuration file are as follows:

- Enter `copy tftp running-config`
- Select a host or network configuration file at the prompt
- Enter the IP address of the TFTP server where the config file is located
- Enter the name of the config file or accept the default name
- Confirm the configuration filename and the server address

Make sure students realize that there are other ways to back up a configuration file. Other methods will be discussed in later sections. It is important for students to understand this process and all the procedures that are explained. It is most important for students to understand that backups are an important part of network management.

### 5.2.4 Managing configuration files using copy and paste

Another way to create a backup copy of the configuration is to capture the output of the `show running-config` command. The output can be copied, pasted into a text file, and saved to create an alternate backup copy. However, the file will need to be edited before it can be used to restore configuration to a router.

To capture the configuration in HyperTerminal, students should perform the following tasks:

- Select **Transfer > Capture Text**
- Specify the name for the text file
- Select **Start**
- Use the `show running-config` command to display the configuration
- Press the **Spacebar** when each `-More-` prompt appears

After the configuration has been displayed, students should select **Transfer > Capture Text > Stop** to stop the capture.

After the capture is completed, the configuration file needs to be edited to remove text that is not required to configure a router. Then it can be pasted back into the router if needed.

The configuration file can be edited from a text editor such as Notepad. The following steps are used to edit the file:

- Select **File > Open**
- Find the captured file and select it
- Click **Open**

The lines that need to be deleted contain the following:

- **show running-config**
- Building Configuration...
- Current Configuration
- -More-
- Any lines that appear after the word End
- At the end of each of the interface sections, students should add **no shutdown**.
- To save the clean version, select **File > Save**.

Before the configuration is restored, any remaining configuration should be removed from the router by issuing the command **erase startup-configuration**. Use the **reload** command to restart the router.

HyperTerminal can be used to restore the configuration:

- Enter global configuration mode.
- Select **Transfer > Send > Text File** in HyperTerminal.
- Select the name of the file.
- Read the lines of the file as they are entered into the router.
- Observe for any errors.
- Press **Ctrl-Z** to exit global configuration mode after the configuration file is entered.
- Use the **copy running-config startup-config** command to restore the startup configuration file.

Students must understand each of the procedures. A backup configuration file is necessary for any network administrator. Explain that minimal down time is required in any network.

Discuss the difference between running configuration and startup-configuration. This concept is very important. Also stress the benefits of comments in the configuration. These comments can explain the function of the various commands. Make sure that the students know that these comment lines begin with an exclamation point (!) and that these lines are not stored in the router.

Some features of HyperTerminal do not work well with the version of HyperTerminal that comes with Windows XP. A free, educational upgrade to HyperTerminal 6.3 can be downloaded from the following website.

<http://www.hillgrave.com/hpte/index.html>

### 5.2.5 Managing IOS images using TFTP

A router may need to have an IOS upgrade or restored. A router should be backed up upon arrival. The IOS image can be stored in a central server with other IOS images to restore or upgrade the IOS into the router and switch. The server should use a TFTP service. The IOS upgrade can be initiated from the privileged EXEC mode with the command `copy tftp flash`. The router will prompt the user to enter the IP address of the TFTP server and then request the filename of the IOS image. If there is not sufficient flash available, the router may prompt the user to erase flash. Flash will be erased before the new image is downloaded.

Students must realize that it is important to maintain current versions of the IOS to eliminate security problems and performance bugs. They also should know that the newer releases are larger and may require flash and RAM upgrades. To ensure a successful transfer, students can ping the TFTP server from the router to test reachability. Stress that when students enter a path name or the name of the IOS, the entry must be exact. If it is not exact, the procedure will not work. One technique is to cut and paste the name of the file from a Windows Explorer directory listing. Explain that this process takes time since the IOS is several megabytes and patience is required. Also point out that the letter e appears when flash is being erased and an exclamation point (!) indicates that a datagram has been successfully downloaded.

### 5.2.6 Managing IOS images using XModem

If the IOS image in flash has been erased or corrupted, the IOS may need to be restored from ROM monitor mode (ROMmon). First, the flash should be examined with the `dir flash:` command. If an image appears to be valid, an attempt should be made to boot from that image. This is done with the `boot flash:` command. If the router boots properly, then the students should determine why the router booted from the ROMmon prompt instead of flash. The `show version` command can be used to check the configuration register. Students can use the `show startup-config` command to see if there is a `boot system` command that instructs the router to use the IOS to monitor ROM.

If the router will not boot properly, a new IOS image will need to be downloaded. The IOS file can be recovered with one of the following methods:

- Use `xmodem` to restore the image through the console.
- Use TFTP from the ROMmon mode to download the image.

To restore the image through the console, the local PC needs to have a copy of the IOS file to restore and a terminal emulation program.

The default console speed of 9600 bps can be used or it can be changed to 115200 bps. This will speed up the download. The console speed can be changed with the `confreg` command.

To restore the IOS image from the PC, students should use the `xmodem` command. The format of the command is `xmodem -c image_file_name`. The `-c` instructs the Xmodem process to use CRC to check for errors during the download. The router then sends a warning message that the bootflash will be erased. Now the Xmodem transfer needs to be started from the terminal emulator. Instruct students to select **Transfer > Send** and then specify the image name and location in the **Send File** popup. Select the xmodem protocol and start the transfer. After the download is complete, the console speed must be changed back to 9600 bps and the configuration register should be changed back to 0x2102. This is done with the `confreg 0x2102` command.

### 5.2.7 Environment variables

The IOS can also be restored from a TFTP session. The fastest way to restore an IOS image from the router is to use TFTP from ROMmon to download the image. This is done with the `tftpdnld` command. The environmental variables provide a minimal configuration. To set a ROMmon environment variable, the name is typed, followed by an equal sign (=) and the value for the variable. All variable names are case sensitive. The minimum variables required to use the `tftpdnld` command are as follows:

- The IP address of the LAN
- The subnet mask
- The default gateway
- The IP address of the TFTP
- The IOS filename on the server

Discuss these procedures with the students and make sure they understand each concept. Also stress the fact that the fastest way to restore an IOS image to the router is to use TFTP from ROMmon to download the image.

[http://www.cisco.com/en/US/customer/products/hw/routers/ps259/products\\_tech\\_note09186a008015bf9e.shtml](http://www.cisco.com/en/US/customer/products/hw/routers/ps259/products_tech_note09186a008015bf9e.shtml)

### 5.2.8 File system verification

There are several commands used to verify the router file system. One is the `show version` command. This command is used to check the current image and available flash. It also verifies the source of the IOS image and the configuration register boot field setting. The `show flash` command is also used to verify the flash system. This command identifies the amount of flash that is available. It also confirms that there is ample space to store a new IOS image. Configuration files may contain boot system commands. These identify the source of the desired boot IOS image. Multiple boot system commands are used to create a fallback sequence to discover and load an IOS. Boot system commands are processed in the order of their appearance in the configuration file.

Discuss the following alternatives with the students:

- NVRAM
- TFTP server
- ROM

Make sure the `boot` commands are reviewed. Stress the importance of familiarity with the bootup procedures.

## Module 5 Summary

Students must be able to manage configuration files and verify the file system with **show** commands before they begin Module 6.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 5 exam.

Students should understand the following main points:

- Identify stages of the router boot sequence
- Identify how the Cisco device locates and loads the Cisco IOS
- Identify the configuration register settings
- Identify the files used by the Cisco IOS and their functions
- Identify the locations on the router of the different file types
- Identify the parts of the IOS name
- Manage configuration files using TFTP
- Manage configuration files using copy-and-paste
- Manage IOS images with TFTP
- Manage IOS images with Xmodem
- Verify the file system using **show** commands

# Module 6: Routing and Routing Protocols

## Overview

When teaching Module 6, remind students that routing refers to the directions that are given to move packets from one network to another. These directions, which are also known as routes, can be dynamically given to the router by another router, or they can be statically assigned to the router by an administrator. Make sure students understand static routing.

### Module 6 Caution

This information contains fundamental terminology that instructors may need to get the students interested in learning about. Make sure students understand this material so that static and dynamic routing can be compared in future lessons.

Students who complete this module should be able to perform the following tasks:

- Explain the significance of static routing
- Configure static and default routes
- Verify and troubleshoot static and default routes
- Identify the classes of routing protocols
- Identify distance-vector routing protocols
- Identify link-state routing protocols
- Describe the basic characteristics of common routing protocols
- Identify interior gateway protocols
- Identify exterior gateway protocols
- Enable Routing Information Protocol (RIP) on a router

## 6.1 Introduction to Static Routing

**Essential Labs:** 6.1.6

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can identify, configure, and verify the use of static and default routes.

**Certification-Level Claim:** Students can evaluate the characteristics of routing protocols.

**Hands-on skills:** none

### 6.1.1 Introduction to routing

Routing is the process that a router uses to forward packets toward the destination network. The routing process is based on the destination IP address of a packet. When routers use dynamic routing, the routing information is learned from other routers. When static routing is used, a network administrator must configure information about remote networks manually. Any network topology changes require the network administrator to add and delete static routes to account for the changes.

Ask students the following questions:

- What is the difference between static and dynamic routing?
- When should a static route be used instead of a dynamic routing protocol?

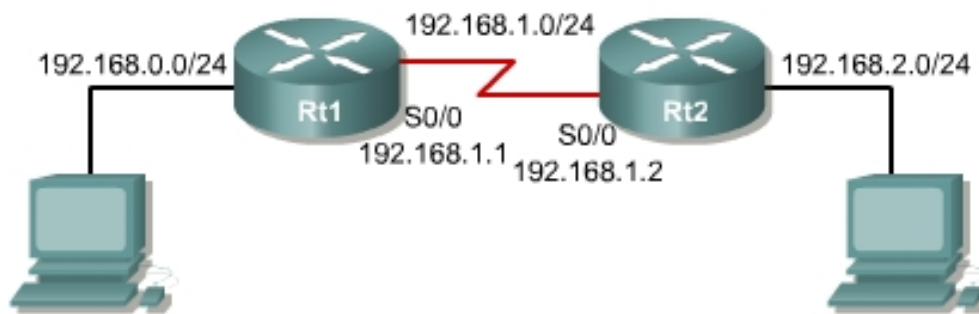
### 6.1.2 Static route operation

Static route operations can be divided into three parts:

- Network administrator configures the route
- Router installs the route in the routing table
- Packets are routed through the static route

Since a static route is manually configured, the administrator must configure the static route on the router with the `ip route` command. The administrator can accomplish this objective in one of two ways. The administrator can specify the outgoing interface or the next-hop IP address of the adjacent router.





From Rt1 either of the following commands will work.

```
Rt1(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
```

This command should be interpreted as “To reach the network 192.168.2.0 that has a subnet mask of 255.255.255.0, the next hop in the path is 192.168.1.2”.

or

```
Rt1(config)#ip route 192.168.2.0 255.255.255.0 s0
```

This should be interpreted as “To reach the network 192.168.2.0 that has a subnet mask of 255.255.255.0, send the packet out interface serial 0/0”.

The administrative distance indicates the trustworthiness of the source of the route. The router assigns an administrative distance of one to static routes by default. The router assumes that if an administrator takes the time to figure out what route the packet should take then this routing information must be very reliable. Only directly-connected routes have a default administrative distance that is trusted more. The default administrative distance for directly-connected devices is zero.

Administrative distance should not be confused with the metric of the route. The metric of the route indicates the quality of a route. When a router decides which route to a particular destination to put in the routing table, it compares the administrative distances of all the routes available to that destination. The router then examines the routes with the lowest administrative distances and chooses the one with the lowest metric.

If the interface that a packet is to be sent to on the next hop is not up, the route will not be installed in the routing table.

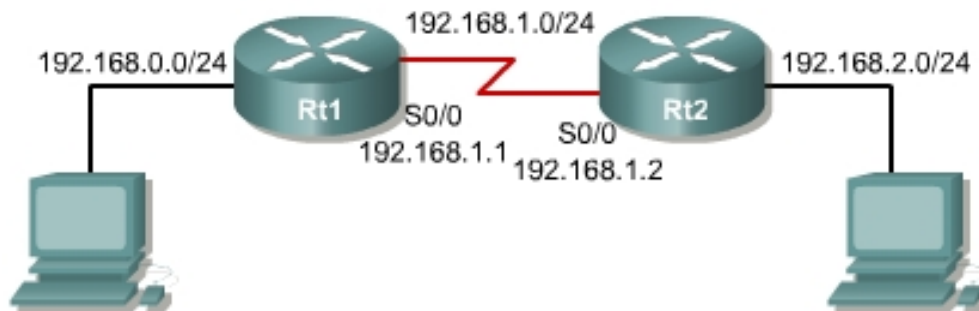
Here is an example of how a default administrative distance of 0 can be changed to an administrative distance of 255:

```
Rt1(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2 255
```

### 6.1.3 Configuring static routes

Use the following steps to configure static routes:

1. Determine all desired destination networks, their subnet masks, and their gateways. A gateway can be either a local interface or a next hop address that leads to the desired destination.
2. Enter global configuration mode.
3. Type the `ip route` command with the address and subnet mask of the destination followed by their corresponding gateway from Step 1. An administrative distance is optional.
4. Repeat Step 3 for as many destination networks as were defined in Step 1.
5. Exit global configuration mode.
6. Save the active configuration to NVRAM by using the `copy running-config startup-config` command.



Here is an example of a route from Rt1 to network 192.168.2.0.

```
Rt1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Rt1(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
Rt1(config)#exit
Rt1#
Rt1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Rt1#
```

All routers must be configured. If Rt2 does not have a route back to network 192.168.0.0, a ping from network 192.168.0.0 will make it to network 192.168.2.0, but will not know how to get back. A relevant TI from CCNA 2 v2.1.4 is 12.1.4.

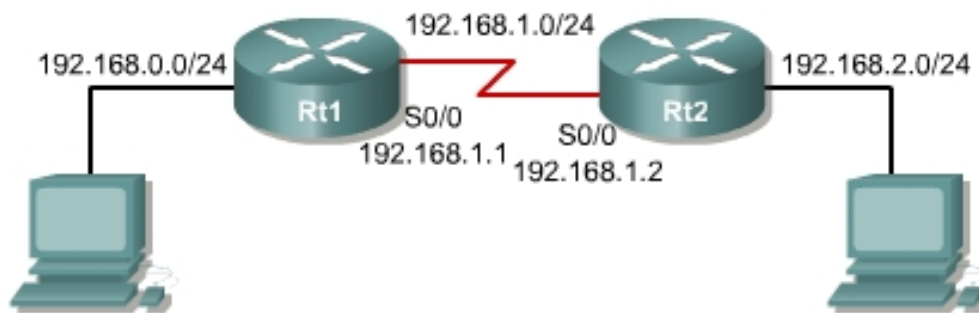
## 6.1.4 Configuring default route forwarding

Default routes are used to route packets with destinations that do not match any of the other routes in the routing table. A default route is actually a special static route that uses the following format:

```
ip route 0.0.0.0 0.0.0.0 [next-hop-address / outgoing interface]
```

Use the following steps to configure default routes:

1. Enter global configuration mode.
2. Type the `ip route` command with `0.0.0.0` for the destination network address and `0.0.0.0` for the subnet mask. The gateway for the default route can be either the local router interface that connects to the outside networks or the IP address of the next-hop router. In most cases, the IP address of the next hop router should be specified.
3. Exit global configuration mode.
4. Save the active configuration to NVRAM with the `copy running-config startup-config` command.



Here is an example for Rt1.

```
Rt1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Rt1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
Rt1(config)#exit
Rt1#
Rt1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Rt1#
```

Remind students of different types of router modes.

## 6.1.5 Verifying static route configuration

After static routes are configured it is important to verify that they are present in the routing table and that routing occurs as expected. The `show running-config` command is used to view the active configuration in NVRAM to verify that the static route was entered correctly.

```

interface Serial0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
no fair-queue
clockrate 56000
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
no ip directed-broadcast
no keepalive
!
ip classless
ip route 192.168.2.0 255.255.255.0 Serial0

```

The **show ip route** command is used to make sure that the static route is present in the routing table.

The output of **show ip route** is as follows.

```

Show ip route output
Rt1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2, E1 - OSPF external type 1, E2 - OSPF external
type 2, E - EGP, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter area, * - candidate default, U - per-
user static route, o - ODR, P - periodic downloaded static route

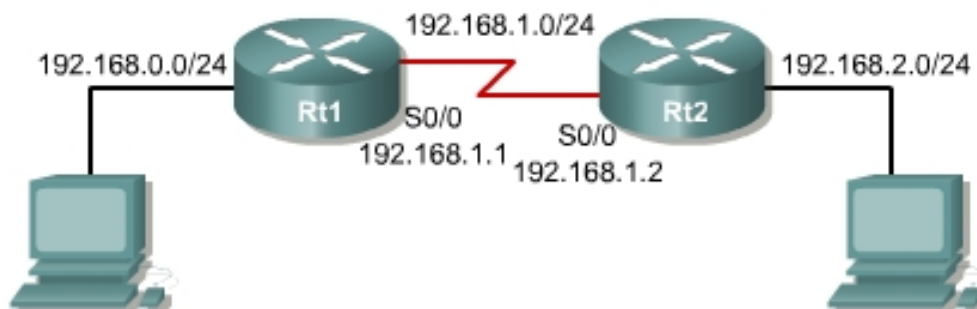
Gateway of last resort is not set

C 192.168.0.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0
S 192.168.2.0/24 is directly connected, Serial0/0
Rt1#

```

### 6.1.6 Troubleshooting static route configuration

The **show interfaces** command can be used to check the state and configuration of the interface that will be used for the route gateway. The **ping** command is used to determine if end-to-end connectivity exists. If an echo reply is not received after a ping, the **tracert** command will be used to determine which router in the route path is dropping the packets.



Here are the outputs of the **show interface**, **ping**, and **traceroute** commands.

```
Rt1#show interfaces s0
Serial0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 00:35:48
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
194 packets input, 12076 bytes, 0 no buffer
Received 194 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
194 packets output, 12076 bytes, 0 underruns
0 output errors, 0 collisions, 5 interface resets
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
Rt1#
Rt1#ping 192.168.2.1
```

Use the escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/32/36 ms
Rt1#
Traceroute command from Rt1.
Rt1#traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
 1 192.168.1.2 16 msec 16 msec *
Rt1#
```

## 6.2 Dynamic Routing Overview

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can evaluate the characteristics of routing protocols.

**Certification-Level Claim:** Students can evaluate the characteristics of routing protocols.

**Hands-on skills:** none

### 6.2.1 Introduction to routing protocols

A routing protocol is a type of communication that is used between routers. A routing protocol allows one router to share information with other routers such as known networks and how close they are to the router. The information a router gets from another router through the routing protocol is used to build and maintain a routing table.

A routed protocol is used to direct user traffic. A routed protocol is a network protocol that provides enough information in its network layer address to allow a packet to be forwarded from one host to another host based on the addressing scheme. The Internet Protocol (IP) is an example of a routed protocol. Students should know the difference between a routed and routing protocol at the end of this TI. Identify the location of each protocol in the OSI model. Ask students the following questions:

- TCP is at which layer?
- IP is at which layer?
- Is the protocol connection-oriented or connectionless?
- RIP, IGRP, EIGRP, and OSPF are at which layer and what is the administrative distance of each?

### 6.2.2 Autonomous systems

An autonomous system is a collection of networks under a common administration that share a common routing strategy. Some routing protocols use an autonomous system to communicate routing information. The routers are configured with the routing protocol and the autonomous system number. Each router can only communicate with other routers within the same autonomous system.

To demonstrate this concept, divide the classroom into groups and tell the students they can only talk to the people in their group. This is similar to a protocol that uses autonomous system numbers. It is possible for routers with different autonomous system numbers and different protocols to communicate if redistribution is used. Redistribution will not be covered in this section.

At this point, students do not have to understand the details of an autonomous system. They just need to understand the basic concepts of an autonomous system. Students do not have enough experience to understand policy-based routing.

### 6.2.3 Purpose of a routing protocol and autonomous systems

The goal of a routing protocol is to fill the routing table with known networks or destinations and the best route to reach these destinations. Although routers can forward packets without a routing protocol configured, using a protocol allows for dynamic updates. The router can be configured with static routes. When static routes are used, the administrator must configure a route for each network. Instruct the students to think of all the networks on the Internet and the different paths to each network. Then instruct the students to think about how fast the Internet changes. A routing protocol will dynamically learn routes to all networks even when the paths change.

The router knowledge needs to reflect an accurate, consistent view of the topology. This view is called convergence. When all routers in an internetwork use the same knowledge, the internetwork is said to have converged. This means all the routers have agreed on the reachable networks.

The purpose of autonomous systems is to segregate the entire network into administrations. If all the routers needed to communicate with all other routers on the Internet, each router would have a tremendous number of routes and would use large amounts of bandwidth to share the routes with the other routers. This is referred to as overhead for the routers. More overhead will increase hardware requirements. When a network is divided into autonomous systems, only the routers inside the local AS receive details about the routing information. Routers in other autonomous systems only need a summary of the routing information. This reduces the number of routes and the amount of routing information that has to be shared, which reduces router overhead. It also improves network stability since routing updates that are caused by topology changes do not have to be shared outside of the local AS. Some routing protocols can be used divide an AS into smaller units to provide the same benefits.

### 6.2.4 Identifying the classes of routing protocols

Most routing algorithms can be classified as one of three basic algorithms:

- Distance vector
- Link state
- Balanced hybrid

Routers will determine which route to take to a given network based on the type of algorithm that is used. Each of the three types has advantages and disadvantages.

### 6.2.5 Distance vector routing protocol features

Distance vector routing algorithms are used to send periodic copies of a routing table. Each router receives a routing table from its directly-connected neighboring routers. RIP sends its entire table every 30 seconds and IGRP sends its entire table every 90 seconds. The algorithm eventually accumulates network distances so that it can maintain a database of

network topology information. This is measured in hop counts, or the number of routers in the path to a destination network.

Distance vector algorithms do not allow a router to know the exact topology of an internetwork. The router only uses hop count to determine the best path. Distance vector algorithms require each router to send its entire routing table to each of its neighbors. This creates network traffic and there is a limit to the number of hops a distance vector routing protocol will use. The RIP maximum hop count is 15 and IGRP is 255. Explain that distance vector routing protocols use the view of neighboring routers to develop their view of the internetwork. The router will use copies of neighboring routing tables to build its routing table.

### 6.2.6 Link-state routing protocol features

The second basic algorithm used for routing is the link-state algorithm. Link-state algorithms are also known as Dijkstras algorithms.

Link-state routing uses the following:

- A topological database
- The SPF algorithm and the resulting SPF tree
- A routing table of paths and ports to each network
- A link-state advertisement (LSA), which is a small packet sent between routers that contains link information

Link-state routing requires more memory. Routers send updates when there is a change in the table. There is less network traffic because the routers are not sending updates every 30 or 90 seconds. The routers in an area elect a Designated Router (DR) and a Backup Designated Router (BDR). When a change is made in the network, the router that notices the change sends an update to the DR. When an update occurs, only the change is sent instead of the entire routing table. The DR then sends the network change to all routers in the area with a multicast.

An important concept to mention is that routers that use a link-state routing protocol develop a common view of the internetwork. A link-state protocol collects links from neighboring routers to create a routing table. Students also need to understand that the updates from the routers contain information about the links. These links can be locally connected or received from other routers. Students also need to know that the updates are partial updates.

## 6.3 Routing Protocols Overview

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can evaluate the characteristics of routing protocols.



**Certification-Level Claim:** Students can evaluate the characteristics of routing protocols.

**Hands-on skills:** none

### 6.3.1 Path determination

Path determination occurs at the network layer, or Layer 3, for traffic that goes through a network cloud. The path determination function enables a router to evaluate the available paths to a destination and to establish the preferred way to handle a packet. This information can be configured by a network administrator or collected through the dynamic processes that operate in the network. Routing protocols help prevent routing loops and use fewer resources. An administrator can configure static routes for all reachable networks. Routers perform two primary functions:

- Path selection
- Switching

During path selection, the routing table is examined to determine the next hop destination of a packet and which interface to use to reach that next hop destination. Switching occurs when a packet is moved to the interface and a frame is created to send the information.

### 6.3.2 Routing configuration

Global and interface parameters must be set when an IP routing protocol is selected. Global tasks include the selection of a routing protocol, either RIP or IGRP, and IP network numbers must be indicated. It is important to check the interface IP address and subnet configuration. A common problem is to assign the wrong IP address or subnet mask. The `network` command is required because it enables the routing process to determine which interfaces will send and receive routing updates. A network statement must be entered for all connected networks. Two common problems are failure to enable the routing protocol or failure to enter all the connected networks.

### 6.3.3 Routing protocols

Examples of IP routing protocols include the following:

- **RIP** – a distance-vector interior routing protocol
- **IGRP** – a Cisco distance-vector interior routing protocol
- **OSPF** – a link-state interior routing protocol
- **EIGRP** – a balanced hybrid distance-vector interior routing protocol
- **BGP** – an exterior routing protocol

Make sure students understand that each routing protocol has advantages and disadvantages. The protocols have different characteristics and were designed for different purposes. In some instances administrators will want to use RIP and other times they will use BGP.

### 6.3.4 IGP versus EGP

Interior routing protocols are designed to be used in a network that is under the control of a single organization. The protocols used in CCNA 2 will be IGPs. The protocols RIP, IGRP, EIGRP, and OSPF are all IGPs. Exterior routing protocols are designed for use between two different autonomous systems. An example of an EGP protocol is Border Gateway Protocol (BGP). BGP is the routing protocol used on the Internet. Interior routing protocols are designed to be used within an autonomous system. BGP is the routing protocol used on the Internet. Interior routing protocols are designed to be used within an AS.

## Module 6 Summary

Before students begin Module 7, they must be able to configure static routes and use the `show ip route`, `ping`, and `traceroute` commands to perform basic network testing.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 6 exam. Formative evaluations of students as they work on the routers may be valuable in this module.

Students should understand the following main points:

- A router will not forward a packet without a route to a destination network.
- Network administrators must manually configure static routes.
- Default routes are special static routes that provide routers with gateways of last resort.
- Static and default routes are configured with the `ip route` command.
- Static and default route configuration can be verified with the `show ip route`, `ping`, and `traceroute` commands.
- How to verify and troubleshoot static and default routes
- Routing protocols
- Autonomous systems
- Purpose of routing protocols and autonomous systems
- The classes of routing protocols
- Distance vector routing protocol features and examples
- Link-state protocol features and examples
- Route determination
- Routing configuration
- RIP, IGRP, OSPF, EIGRP, and BGP routing protocols
- Autonomous systems and IGP versus EGP
- Distance vector routing
- Link-state routing

# Module 7: Distance Vector Routing Protocols

## Overview

When teaching module 7, emphasize both skills development and conceptual understanding of the routing protocols RIP and IGRP. Students must master the basic routing skills and concepts from this module to be successful in CCNA 3.

Before students begin this section, they should be able to connect to Cisco routers and switches with serial or Ethernet cables, console and Telnet into a router, and configure TCP/IP on router interfaces

### Module 7 Caution

Many students do not have prior experience with routing protocols. Encourage the students to spend plenty of time in the labs and to experiment with RIP. Since the labs are complex, students may require additional time, which may affect the availability of lab equipment. Provide guidance on how to follow an effective, well-documented, and patient troubleshooting strategy, since students may need to troubleshoot their labs. If the lab IOS does not support IGRP, instructors should use EIGRP and emphasize how it is similar to IGRP. EIGRP is covered in CCNA 3.

Students who complete this module should be able to perform the following tasks:

- Describe how routing loops can occur in distance vector routing
- Describe several methods used by distance vector routing protocols to ensure that routing information is accurate
- Configure RIP
- Use the `ip classless` command
- Troubleshoot RIP
- Configure RIP for load balancing
- Configure static routes for RIP
- Verify RIP
- Configure IGRP
- Verify IGRP operation
- Troubleshoot IGRP

## 7.1. Distance Vector Routing

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can identify, analyze, and show how to rectify inherent problems associated with distance vector routing protocols.

**Certification-Level Claim:** Students can troubleshoot and configure routing protocols based on user requirements.

**Hands-on skills:** none

### 7.1.1 Distance vector routing updates

Distance vector routing protocols require routers to forward their entire routing table when passing along updates. Convergence is a step-by-step process with distance vector routing protocols. This means that routing table information is forwarded to neighbor routers, which continue to forward the information to their neighbors. This is contrasted with link-state routing protocols, which forward their routing tables out to all routers in their area. These routing tables include information about the total cost of a route and the logical address of the first router on the path to each network contained in the table.

Routers need to update the information in their routing tables to continuously make good path determination decisions. Periodically, changes in a network will affect the decisions made by a router. For example, a router may be taken off line for upgrades or repairs or an interface on a router may go down. If routers are not aware of the changes that have occurred in a network, they may switch packets to interfaces that are no longer connected to the best route.

Distance vector routing protocols typically send out updates at certain time intervals such as every 30 seconds for RIP. Sometimes distance vector routing protocols initiate updates when topology changes occur. For example, IGRP sends out flash updates sooner than its standard update interval of 90 seconds.

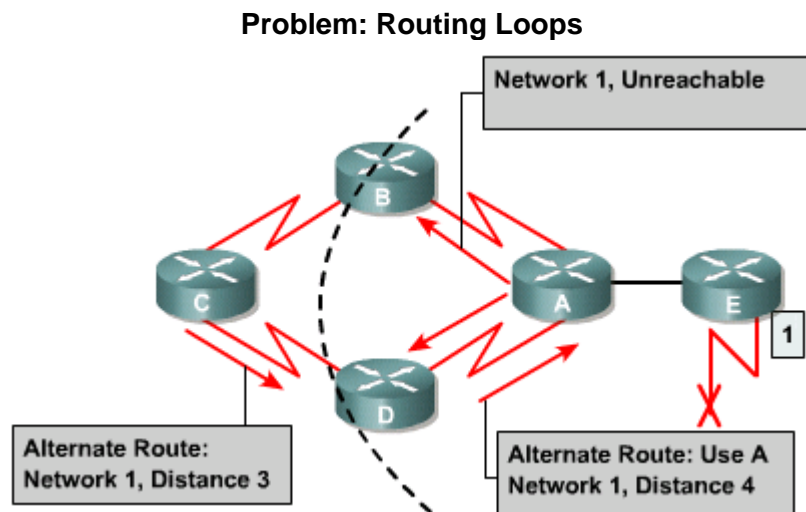
### 7.1.2 Distance vector routing loop issues

Routing loops can occur if slow convergence on a network causes inconsistent routing entries. If a network goes down, this information may not get propagated across the network quickly enough. As a result, a router may develop an incorrect view of the network and send out this incorrect information.

Use the following example in class:

- Just before the failure of Network 1, all routers have consistent knowledge and correct routing tables. The network is said to have converged. Assume for the remainder of this example that for Router C, the preferred path to Network 1 is by way of Router B and the distance from Router C to Network 1 is three.

- When Network 1 fails, Router E sends an update to Router A. Router A stops routing packets to Network 1, but Routers B, C, and D continue to route packets because they have not yet been informed of the failure. When Router A sends out its update, Routers B and D stop routing to Network 1. However, Router C has not received an update. Router C still tries to reach Network 1 through Router B.
- Now Router C sends a periodic update to Router D, which indicates a path to Network 1 through Router B. Router D changes its routing table to reflect this incorrect information and propagates the information to Router A. Router A propagates the information to Routers B and E and the process continues. Any packet that is destined for Network 1 will now loop from Router C to B to A to D and back again to C.



Convergence is when all routers have the same information about the network. Convergence is a by-product of the routing updates that are sent out based on the routing protocol used on a router. If updated information does not reach all routers in a network quickly enough, then incorrect routing information may be sent out by routers that have not received the updates, which will replace the correct information in other routers.

In the example, Router C sends out an update to neighbor routers that incorrectly indicates that a route to Network 1 exists. This is a timing issue. Router C sends out updates before its neighbors have a chance to send out their newly updated information. Therefore, the accurate information is replaced by inaccurate information, which creates a routing loop.

A kinesthetic activity may be helpful to students to get a mental picture of how this process occurs. Instruct students to write their updates on paper and reenact the scenario from the figure and description.

### 7.1.3 Defining a maximum count

The previous section described a situation in which slow convergence created the impression that a fictitious path to a network existed, which leads to a routing loop. Routing loops have a packet that circles a network, uses up bandwidth, and never reaches its destination. Distance vector algorithms are designed to prevent these loops by defining a maximum hop count. This value is known as a routing metric. A metric is the criteria used by a router to determine the best path to a destination network. Metrics vary for different protocols. Some protocols such as RIP use only the metric of hop counts. Other routing protocols may use bandwidth, delay, and other factors. If the only metric used by a routing protocol is hop count then a router makes its path determination decisions based on the lowest number of routers that a packet will have to pass through to reach its destination.

The maximum hop count value defines how many routers a packet can pass through before the destination network is unreachable. Each time a packet passes through a router the distance number is increased. When the default or defined maximum is reached the network is considered unreachable and the looping ceases. A non-technical example is a timed test. If someone takes a timed test they have a predefined amount of time to complete it. When the maximum amount of time has been reached, the test ends even if some questions have not been answered.

### 7.1.4 Eliminating routing loops through split horizon

Another possible source for a routing loop occurs when incorrect information that has been sent back to a router contradicts the correct information that it sent. The following example explains how this problem occurs:

1. Router A passes an update to Router B and Router D that indicates that Network 1 is down. Router C transmits an update to Router B that indicates that Network 1 is available at a distance of four, by way of Router D. This does not violate split-horizon rules.
2. Router B incorrectly concludes that Router C still has a valid path to Network 1 at a less favorable metric. Router B sends an update to Router A to inform Router A of the new route to Network 1.
3. Router A now determines that it can send to Network 1 by way of Router B, Router B determines that it can send to Network 1 by way of Router C, and Router C determines that it can send to Network 1 by way of Router D. Any packet that is introduced into this environment will loop between routers.
4. Split-horizon attempts to avoid this situation. As shown in Figure [1], if a routing update about Network 1 arrives from Router A, Router B or Router D cannot send information about Network 1 back to Router A. Split-horizon reduces incorrect routing information and reduces routing overhead. [2]

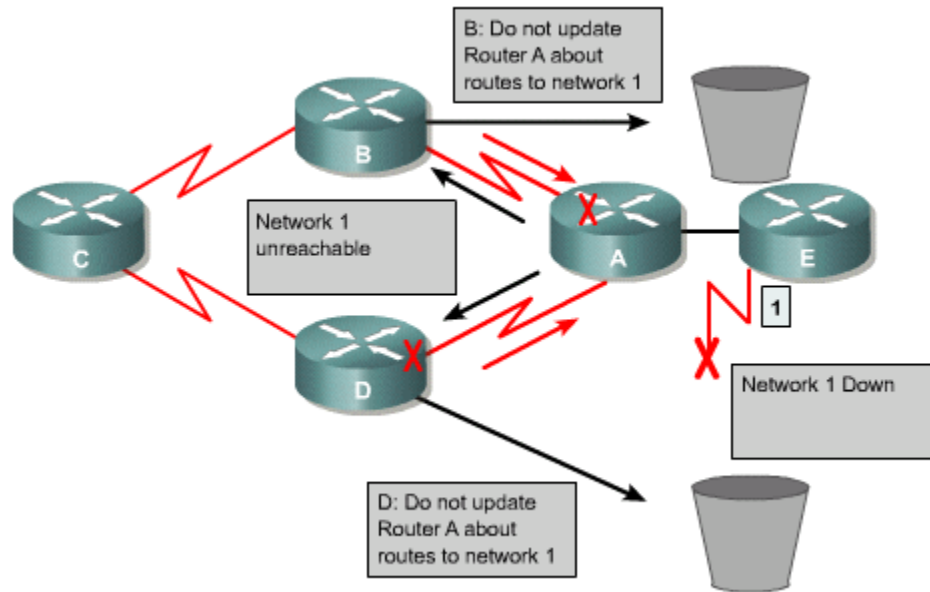


Figure [1]: Routing Update

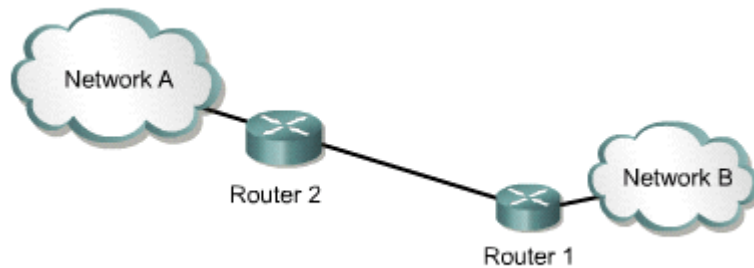


Figure [2]: Split Horizon

Split horizon is another mechanism to help prevent routing loops. Split horizon does not allow the originator of network information to receive updates about the network from another router. This prevents the originator of correct information from being influenced by the incorrect information of another router.

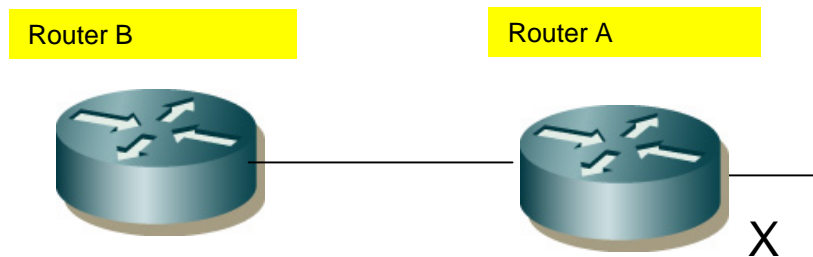
Use the figure in this section for reference. If Router 2 sends out an update to Router 1 about the status of Network A, it cannot receive a report back from Router 1 about Network A.

From the description in the curriculum, which is included above, if split horizon were in use in Step 2, Router A would have ignored information about Network 1 from Router B. More specifically, Router B would not have attempted to update Router A about that particular network in the first place because Router A originally informed Router B about the status of Network 1. Refer to Figure [1] Routing Update for a graphical representation of this process.



## 7.1.5 Route poisoning

Route poisoning is another process used by routers to prevent routing loops. Briefly review the fact that routing loops are typically the result of slow convergence. The loops are interrupted when maximum hop counts are defined so that packets that are caught in loops are eventually dropped. Route poisoning is when the distance or hop count of a route is changed to 16, or 1 higher than the maximum number allowed, which makes it unreachable from the perspective of the routers. This process of route poisoning results in an update about the poisoned route that is sent out to neighboring routers before the routing update time has been reached.



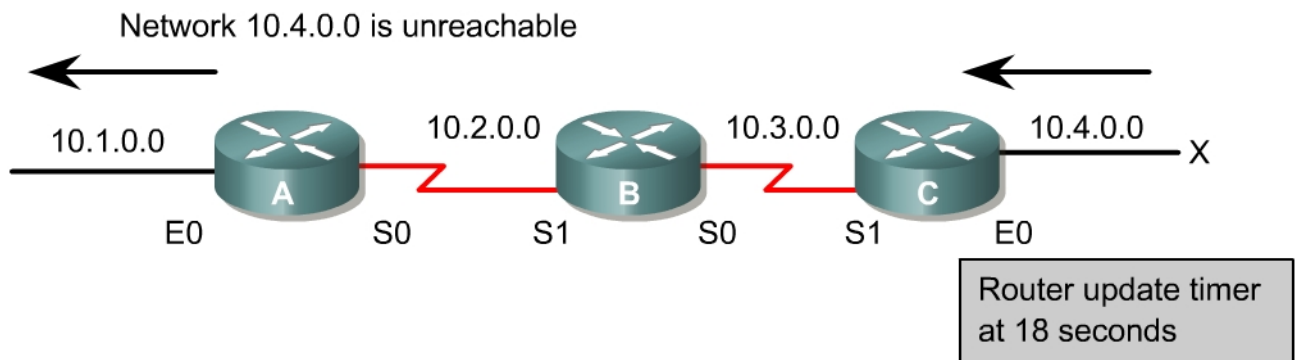
Reference the graphic in this section. When Router A determines that Network X is down, it poisons the route in its table. To do this, it sets the hop count to Network X to one more than the maximum. It then sends a poison update to Router B regardless of the time schedule for routing updates. This does not send the entire table. It only sends the route poisoning. This single change, which indicates that Network X is now unreachable, is quickly propagated through the network. This speeds convergence and reduces the likelihood that a loop will develop.

## 7.1.6 Avoiding routing loops with triggered updates

Routing table updates are automatically sent out at specific time intervals by distance vector routing protocols. As discussed earlier, slow convergence can create a scenario in which routers incorrectly think a route to a network is available, which results in a routing loop. Triggered updates such as route poisoning help prevent these routing loops by sending out updates when topology changes occur without waiting for the update time to be reached. This speeds up convergence in relationship to network topology changes.

Reference the graphic in this section. A triggered update would occur if Network X went down. Router C would detect the change, update its routing table, and then send out an update to Router B even though its update timer is set at 18. IP RIP would send out table updates at 30 seconds and IGRP would send them out at 90 seconds. This triggered update would poison the route until the holddown timer, which is discussed in the next section, has expired.

Make sure students understand that a triggered update is generated by the router that detects a topology change and sends the update to its neighbors.



### 7.1.7 Preventing routing loops with holddown timers

Holddown timers are used to prevent update messages from reinstating inaccessible routes. When a router receives an update that indicates that a network is unreachable, it starts a hold-down timer. While the hold-down timer is running, the router will not accept any updates about the inaccessible route unless the update comes from the originator of the triggered update or from a router reporting a better metric to the inaccessible network.

If a router receives routing update information from a router other than the originator of the triggered update that says it has a route to the inaccessible network with a lower metric than the original metric, the router ignores the update information while the holddown timer is still in effect.

Holddown timers are used to allow updates about bad routes to be propagated. Routers that have already received the information will not accept update information about the bad route from neighbor routers that may not know that it is inaccessible.

Students may need some additional help with distance vector routing protocols. Several of the topics will be discussed later in the RLO. It may be helpful to discuss related concepts such as holddown timers, route poisoning, and triggered updates in a combined lesson with the entire class. Group discussions about how these features fit together to help prevent routing loops may be helpful to students.

## 7.2 RIP

**Essential Labs:** 7.2.2, 7.2.6, 7.2.7, and 7.2.9

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can configure, verify, analyze, and troubleshoot simple distance vector routing protocols.

**Certification Level Claim:** Students can troubleshoot and configure routing protocols based on user requirements.

**Hands-on skills:** none

## 7.2.1 RIP routing process

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. By default, the maximum hop count for RIP is 15 and routing updates are broadcast every 30 seconds. If RIP routes are received that would increase the metric to a number higher than 15 hops, the network is considered unreachable and the route is discarded. RIP also has other features that are used by distance vector routing protocols such as split horizon and hold-down mechanisms to prevent incorrect routing information from being propagated.

## 7.2.2 Configuring RIP

Basic RIP configuration consists of two steps:

1. Enable the routing protocol
2. Identify the directly connected networks, or the networks to advertise

The global configuration command `router rip` is used to enable RIP as the routing protocol. The `network network address` command allows the identification of directly-connected networks that will participate in the routing process. When the basic configuration of RIP is complete, regular updates are sent every 30 seconds and triggered updates are sent upon notification of metric changes.

The following is an example of RIP configuration:

- `BHM(config)#router rip` – selects RIP as the routing protocol
- `BHM(config-router)#network 1.0.0.0` – specifies a directly connect network
- `BMH(config-router)#network 2.0.0.0` – specifies a directly connect network

Notice that the network statements configured under the RIP protocol are classful addresses. Students commonly configure the network command by using the IP address of the subnet. The IOS will change this to the classful network address.

The router interfaces associated with the directly connected networks will participate in the routing process. These interfaces will send and receive routing updates.

RIP can be further customized through the use of some optional configuration parameters:

- Apply offsets to routing metrics
- Adjust timers
- Specify a RIP version
- Enable RIP authentication
- Run IGRP and RIP concurrently
- Disable the validation of source IP addresses
- Enable or disable split horizon

### 7.2.3 Using the ip classless command

The `ip classless` command allows packets that are bound for an unknown subnet to be routed out the same interface as other known subnets in the same range of addresses. IP classless only affects the operation of the forwarding processes in IOS. It does not affect the way the routing table is built.

When the `no ip classless` command is used, a packet bound for an unknown subnet will be dropped even if a route to a subnet in the same address range exists. The basic principle of classful routing is that if one part of a major network is known, but the subnet toward which the packet is destined within that major network is unknown, the packet is dropped. One aspect of this rule that may confuse students is that the router will only use the default route if the destination major network does not exist in the routing table at all.

### 7.2.4 Common RIP configuration issues

RIP is a distance-vector routing protocol and like all distance-vector protocols they are slow to converge and have to deal with routing loops and counting to infinity. To reduce the routing loops and counting to infinity, RIP uses the following mechanisms:

- Split horizon
- Poison reverse
- Holddown counters
- Triggered updates

RIP permits a maximum hop count of 15 and any destination greater than 15 hops away is tagged as unreachable. This maximum hop count prevents counts to infinity and endless network routing loops. The split horizon rule prevents information about a route from being sent out the same interface from which it was originally received. Split horizon is used to avoid the creation of routing loops due to multiple routers that advertise routes to each other about the same network. The `no ip split-horizon` command can be used to disable split horizon.

Hold-down timers are used to define the amount of time that a possible down route will be held and routes with higher metrics to the same network will not be accepted. The default hold-down time is 180 seconds, which is 6 times the regular update period. When a route goes down, the hold-down timer is started. During this time period, a route with a higher metric than the original metric will not be accepted. If the original route comes back up or a route with a lower metric than the original metric is advertised, they will be accepted immediately. The hold-down timer will reduce routing loops but it may also slow convergence. The `timers basic 30 90 180 540` router configuration command can be used to adjust the basic timers. The holddown is the third number.

RIP updates are broadcast by default every 30 seconds. This can be increased to reduce network congestion or decreased to improve convergence with the `timers basic 30 90 180 540` command. The update timer is the first number listed. In some instances, it may be necessary to avoid the advertisement of routing updates out a specific interface. This can be accomplished with the `passive-interface interface` router configuration command. For RIP to function in a non-broadcast environment, neighbor relationships must be configured. This can be accomplished with the `neighbor ip address` router configuration

command. The RIP version can also be changed with the `version [1 | 2]` router configuration command. Other variations of this command may be placed on the interface to specify which version of packets to send and receive.

## 7.2.5 Verifying RIP configuration

The `show ip protocol` and the `show ip route` commands can be used to verify the configuration of RIP. The `show ip protocol` command displays information about all of the IP routing protocols that are used on the router. This command can be used to verify that RIP is configured, interfaces are correctly sending and receiving RIP updates, and that the router is advertising the correct networks. The basic timers, filters, and version can also be verified with the `show ip protocol` command. The `show ip route` command can be used to verify that RIP routes are received. These routes will be identified by an "R", which indicates that they were learned through RIP.

## 7.2.6 Troubleshooting RIP update issues

Some common RIP configuration errors include incorrect network statements, discontinuous subnets, and split horizons. These RIP update issues can be identified with some basic `show` and `debug` commands. The `debug ip rip` command enables rip debugging and will display all of the rip updates as they are sent and received. The following is an example of the output of the `debug ip rip` command:

```
LAB-A#debug ip rip
RIP protocol debugging is on
LAB-A#
RIP: ignored v1 update from bad source 223.8.151.1 on Ethernet0
RIP: sending v1 update to 255.255.255.255 via Ethernet0
(192.5.5.1)
  network 204.204.7.0, metric 3
  network 223.8.151.0, metric 3
  network 201.100.11.0, metric 1
  network 219.17.100.0, metric 2
  network 199.6.13.0, metric 2
  network 205.7.5.0, metric 1
  network 210.93.105.0, metric 4
RIP: sending v1 update to 255.255.255.255 via Ethernet1
(205.7.5.1)
  network 204.204.7.0, metric 3
  network 223.8.151.0, metric 3
  network 201.100.11.0, metric 1
  network 219.17.100.0, metric 2
  network 192.5.5.0, metric 1
  network 199.6.13.0, metric 2
  network 210.93.105.0, metric 4
RIP: sending v1 update to 255.255.255.255 via Serial0
(201.100.11.1)
  network 192.5.5.0, metric 1
  network 205.7.5.0, metric 1
RIP: ignored v1 update from bad source 219.17.100.1 on Ethernet0
RIP: received v1 update from 201.100.11.2 on Serial0
  204.204.7.0 in 2 hops
  223.8.151.0 in 2 hops
```

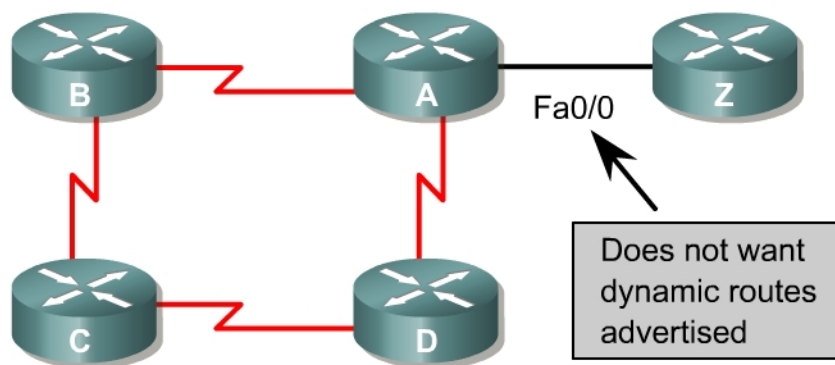
```
219.17.100.0 in 1 hops
199.6.13.0 in 1 hops
210.93.105.0 in 3 hops
```

Other commands that can be used to troubleshoot RIP update issues include the following:

- show ip rip database
- show ip protocols
- show ip route
- debug ip rip
- show ip interface brief

### 7.2.7 Preventing routing updates through an interface

The **passive interface** command prevents routing updates from being sent out a particular interface. In the graphic, Router Z interface Fa0/0 is not allowed to send router updates to Router A. This may be implemented for a variety of reasons. One reason might be that the administrator of Router Z does not want information about the internal network to be sent out to other routers. If Router Z is a stub network, the administrator of Router A may prevent routing updates from being sent to Router Z since there is one way in and one way out. Students must understand that routes will still be learned through this interface. They also need to know that the network that this interface is connected to is advertised if a network statement is configured for that network.



Command

```
Router Z (config-router) #passive-interface Fa0/0
```

### 7.2.8 Load Balancing with RIP

Load balancing is the process of routing packets over multiple equal-cost paths to increase throughput. RIP can load balance over as many as six equal-cost paths, although four is the default. Packets are sent “round robin” over the equal-cost paths, this means that the equal-cost paths are used in turn. Since the metric for RIP is hop count, equal-cost paths indicate that a network can be reached through multiple paths that have the same hop count.

This does not consider the bandwidth of each link. So while load balancing may allow packets to travel multiple paths to reach a destination, huge bandwidth differences among equal-cost paths could actually slow throughput.

### 7.2.9 Load balancing across multiple paths

A router may have multiple paths to a given destination network. If these paths have different metrics the router will use the route with the best metric to forward packets. If multiple routes have the same metric associated with them, the router will use load balancing to spread out the traffic that is forwarded to a particular network. This helps reduce traffic on a given route to speed up communications. Load balancing is enabled by default on routers that use RIP and IGRP. With the exception of BGP, IP routing protocols route to four parallel routes by default. The administrator also has the option of load balancing on a per-packet or per-destination basis. A per-destination basis implies that all packets headed for a particular host on the network during a given communication session will take the same path.

Students should be comfortable with the term “round-robin” load balancing. This means that packets will be equally shared between the equal paths. This is done by alternating the packet output between the interfaces for each of the paths. The students should also understand that this does not equally balance the traffic between the paths. This is because the packets are of various sizes. So even though the same number of packets will be forwarded out of the interfaces, the amount of traffic will vary.

### 7.2.10 Integrating static routes with RIP

Static routes are user-defined routes that force packets to take a specific path. These are usually used when a dynamic route cannot be built, the overhead of dynamic routing is not desirable, or if another route for fault tolerance is desired. A static route can be configured on the router with the `ip route` command and removed with the `no ip route` command. These routes can then be redistributed or shared through the dynamic routing protocol with the `redistribute static` command.

## 7.3 IGRP

**Essential Labs:** 7.3.5 and 7.3.6

**Optional Labs:** 7.3.8

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can configure, verify, analyze, and troubleshoot simple distance vector routing protocols.

**Certification-Level Claim:** Students can troubleshoot and configure routing protocols based on user requirements.

**Hands-on skills:** none

### 7.3.1 IGRP features

IGRP is a Cisco proprietary distance-vector interior gateway routing protocol. Distance vector routing protocols mathematically compare routes to determine the best path. IGRP was designed to take advantage of the simplicity of RIP and adds other metrics for best path selection and better scalability. The metrics available with IGRP are bandwidth, delay, load, reliability, and maximum transmission unit (MTU). These metrics can be used to make better mathematical decisions about best paths than the hop count metric used by RIP. By default, bandwidth and delay are the two metrics that are used and the others are set to zero. IGRP shares its routing information through the use of timed updates every 90 seconds.

Draw an example on the board to demonstrate how IGRP can make better routing decisions than RIP. There are three important points to emphasize:

- IGRP is Cisco proprietary. If students can select which routing protocols to use, the internetwork will have to be all Cisco devices for IGRP to be chosen.
- The default update time of IGRP is 90 seconds and the updates are broadcast.
- The default algorithms of IGRP are bandwidth and delay. The others can be used if the algorithm is changed. MTU is only exchanged in the update. It is not used in any calculation.

One additional item to note is that Cisco offers more support for EIGRP than IGRP. Many of the newer releases of IOS do not support IGRP.

### 7.3.2 IGRP metrics

IGRP uses several metrics to calculate the overall routing metric of each route:

- **Bandwidth** – the lowest bandwidth value in a path
- **Delay** – the cumulative interface delay along a path
- **Reliability** – the reliability between source and destination, determined by the exchange of keepalives
- **Load** – the load on a link between a source and a destination based on bits per second
- **MTU** – the maximum transmission unit value of a path

The `show ip protocol` command is used to display parameters, filters, and network information about the routing protocol used by a router. Each metric has a corresponding K value or weight. By default, only K1 and K3 are set to one. These represent the K values for bandwidth and delay. The K values of the other metrics are set to zero. By default, only bandwidth and delay are used to determine the composite metric or routing metric of each route. This use of multiple components to calculate a composite metric provides greater accuracy than the RIP hop-count metric to choose the best path.

The `show ip route` command displays the composite IGRP metric for a given route in brackets with the administrative distance. A link with higher bandwidth will have a lower metric. A link with lower cumulative delay will have a lower metric.



The lower the metric is, the better the route. Make sure that students understand that the default metrics for IGRP are bandwidth and delay. The other metrics can be used but are not used by default. Allow the students to configure IGRP on a mesh network and adjust the metrics to see how the routing table is changed. Students should also be instructed to trace the path to a network before and after the metric changes to verify the different path selection.

### 7.3.3 IGRP routes

IGRP advertises three types of routes:

- Interior
- System
- Exterior

Interior routes are defined as routes between subnets that are connected to the same router interface. System routes are routes within the same autonomous system. These routes are derived from directly connected networks and through routes learned from other IGRP routers. System routes do not contain subnet information. Exterior routes are routes between autonomous systems. A gateway of last resort can be used to transfer information to a destination outside of a local autonomous system.

Describe the graphic included in the TI in depth. Explain the concepts of interior routes and multiple subnets on the same router interface. Autonomous systems should also be explained.

### 7.3.4 IGRP stability features

Features designed to enhance the stability of IGRP consist of holddowns, split horizons, and poison-reverse updates. Holddowns are used to prevent regular update messages from reinstating a route that is down. This is done through the lack of regularly scheduled update messages. If a router does not receive an update about a particular route, it marks that route as possibly down. Split horizons are designed to prevent routing loops with the rule that routing information is not sent back in the direction from which it was learned. This prevents routing loops between adjacent routers. Poison-reverse updates are necessary to avoid larger routing loops. An increase in metric may indicate a routing loop, so poison-reverse updates are sent to place the route with the increasing metric in holddown. IGRP sends out poison-reverse updates when the route metric has increased by a factor of 1.1 or more.

The timers associated with IGRP include update, invalid, hold-down, and flush timers. The update timer indicates how often routing updates will be sent, the default for IGRP is 90 seconds. The invalid timer is the amount of time that IGRP will wait before it declares a route invalid. The default for IGRP is 270 seconds, which is 3 times the update period. The hold-down variable specifies the holddown period. During this period the information about better routes is suppressed, even though the route in holddown is marked as inaccessible and advertised as unreachable. When the holddown time has expired, routes advertised by other routers are accepted. The default holddown time is greater than three times the update time. The flush timer indicates the amount of time that a route should remain in the routing table before it is flushed. This time should be at least as long as the holddown and invalid times combined. This will allow the proper holddown phase, otherwise the route may be flushed and new routes may be accepted prematurely. The default flush timer is seven times the update time. The `show ip protocol` command should be used to view the timers and then timers should be changed and viewed again.

The `debug ip igrp events` command can be used to verify that the timers affect routing updates. Have the students configure IGRP on the lab topology.

### 7.3.5 Configuring IGRP

To enable IGRP routing use the `router igrp as-number` global configuration command. To disable IGRP routing use the `no router igrp as-number` command.

```
RouterA(config)#router igrp as-number
RouterA(config-router)#
RouterA(config)#no router igrp as-number
RouterA(config)#
```

To identify which networks will participate in the IGRP routing process, use the `network network-address` router configuration command. To remove a network from the IGRP routing process, use the `no network network-address` command.

```
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config)#router igrp 101
RouterA(config-router)#no network 192.168.1.0
```

The autonomous system number is used to identify the router to other IGRP routers and to tag routing information. Have the students configure IGRP on the lab topology.

### 7.3.6 Migrating from RIP to IGRP

With the creation of the IGRP in the early 80s, Cisco Systems was the first company to solve the problems associated with RIP. IGRP was designed to have a greater maximum hop count, which gave it more scalability for larger companies. IGRP uses multiple metrics to determine the best path, bandwidth, and delay, as opposed to the hop count metric used by RIP. As a result of these improvements, IGRP enabled many large, complex, and topologically diverse internetworks to be deployed. Have the students configure the lab topology with RIP and then migrate to IGRP. Make sure that students understand that RIP is still the most implemented routing protocol in smaller internetworks. Also, emphasize that IGRP can only be used in a fully Cisco environment.

### 7.3.7 Verifying IGRP Configuration

The following commands and available switches can be used to verify the configuration of IGRP:

- show interface
- show ip protocol
- show ip route
- show running-config

The `show interface` command can be used to verify issues that are specifically related to the interface configuration such as the ip address, physical connectivity, and keepalives. The `show ip protocol` command should be used to verify that routing protocols are correctly configured. This command can be used to view the routing protocols enabled on the router,

the networks advertised, timer values, and other routing protocol-specific information. The `show ip route` command displays the routing table and lists the next hop to all known networks, how the route was learned, the metric, and other route specific information. The `show run` command can be used to verify the running configuration. Have the students verify proper operation of IGRP on the lab topology.

### 7.3.8 Troubleshooting IGRP

Most of the IGRP configuration errors involve a bad network statement, discontinuous subnet, or incorrect autonomous system number. The following commands are used to troubleshoot IGRP:

- `show ip protocols`
- `show ip route`
- `debug ip igrp events`
- `debug ip igrp transactions`
- `ping`
- `trace`

Both the `debug ip igrp events` and `debug ip igrp transactions` commands can be used to verify that routing information is being passed between routers. The `ping` command can be used to test network connectivity. The `trace` command can be used to locate pinpoint delay or connectivity issues. Have the students take a break and place several IGRP problems on the lab topology. When the students return from the break, instruct them to troubleshoot the topology and correct any problems they find. Emphasize the fact that the `show run` command, which makes it easy to troubleshoot problems in a lab, may not be very effective in real situations. The `show run` command should be used to verify configuration changes.

## Module 7 Summary

Before students begin Module 8, they must be able to configure and troubleshoot RIP and IGRP by themselves.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 7 exam. Formative skill assessments such as timed competitions to see who can get hands-on or e-Lab routing to work the fastest should be used. The emphasis of any assessment should be on the ability to demonstrate mastery.

Students should understand the following main points:

- How routing information is maintained through distance vector protocols
- How routing loops occur in distance vector
- How to define a maximum to prevent count to infinity
- How to eliminate routing loops through split horizon
- Route poisoning
- How to avoid routing loops with triggered updates
- How to prevent routing loops with holddown timers
- How to prevent routing updates through an interface
- Load balancing across multiple paths
- RIP process
- RIP configuration
- The `ip classless` command
- Common RIP configuration issues
- Load balancing with RIP
- How to integrate static routes with RIP
- How to verify RIP configuration
- IGRP features
- IGRP metrics
- IGRP routes
- IGRP stability features
- How to configure IGRP

- How to migrate RIP to IGRP
- How to verify IGRP configuration
- How to troubleshoot IGRP

# Module 8: TCP/IP Suite Error and Control Messages

## Overview

The main goal of Module 8 is for students to learn how the IP protocol uses the ICMP protocol to provide control messages to hosts on a network. IP does not have the facilities to send error messages. It uses ICMP to send, receive, and process error and control messages.

### Module 8 Caution

Error and control messaging is an important aspect of TCP/IP. Make sure the students understand that ICMP is the protocol that handles these functions for the TCP/IP suite. If time is an issue, this module can be used as a reference for other modules when students encounter different ICMP error messages in their labs and in their use of programs such as browsers and e-mail.

Students who complete this module should be able to perform the following tasks:

- Describe ICMP
- Describe the ICMP message format
- Identify ICMP error message types
- Identify potential causes of specific ICMP error messages
- Describe ICMP control messages
- Identify a variety of ICMP control messages that are used in networks
- Determine the causes for ICMP control messages

## 8.1 Overview of TCP/IP Error Message

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** 8.1.1, 8.1.2, 8.1.4, 8.1.5, 8.1.6, and 8.1.8

**Optional TIs:** 8.1.3, 8.1.7, and 8.1.9

**Course-Level Claim:** Students can describe the operation of ICMP and identify the reasons, types, and format of associated error and control messages.

**Hands-on skills:** none

### 8.1.1 ICMP

IP is considered a “best effort” or unreliable method for the delivery of network data. If the data does not reach its destination, the sender is not notified that the transmission has failed. ICMP is the component of the TCP/IP protocol stack that addresses the limitations of IP. ICMP does not overcome the unreliability issues in IP but ICMP does allow for testing. Reliability must be provided by upper layer protocols. Explain the difference between a guaranteed method and a best effort. This is a good time to show students how a successful ICMP works. Introduce problems into the lab setup to demonstrate how ICMP relays messages in a network. Explain that ICMP is a Layer 3 protocol of the TCP/IP suite. It is not an IP packet. It uses the IP addressing scheme but has a different packet format than IP.

### 8.1.2 Error reporting and error correction

ICMP is an error reporting protocol for IP. When datagram delivery errors occur, ICMP is used to report these errors back to the sender of the datagram.

This is an excellent opportunity to show the students this procedure in the lab setup. They should be shown that ICMP does not correct the encountered network problem. ICMP just reports on the status of the delivered packet to the sender. Its function is not to propagate information about network changes.

### 8.1.3 ICMP message delivery

ICMP is a message protocol for TCP/IP protocol suite. ICMP messages are encapsulated as data in ICMP packets in the same way that IP data is delivered. ICMP messages have their own header information. They are subject to the same failures as any other data. The students should realize that ICMP is a Layer 3 protocol that does not use IP packets. ICMP uses IP addressing but has a different structure than an IP packet. Show the students that this scenario could generate more error reports and cause increased congestion on an already ailing network. For this reason, errors created by ICMP messages do not generate their own ICMP messages. Stress to the students that it is possible to have a datagram delivery error that is never reported back to the sender of the data.

### 8.1.4 Unreachable networks

Network communications depend on certain basic conditions:

- The sending and receiving devices must have the TCP/IP protocol configured.
- This includes a correct IP address and subnet mask.
- A default gateway must be set if data will go outside the LAN.
- Devices must be placed to route the data.
- The router must be configured correctly and the correct routing protocol must be used.

If these conditions are not met, communication cannot occur. Instruct the students to discuss problems that could cause a network to be unreachable.

### 8.1.5 Using ping to test destination reachability

The ICMP protocol can be used to test the availability of a destination. If a destination receives the ICMP echo request, it formulates an echo reply to send back to the source. If the sender receives the echo reply, this confirms that the destination can be reached. The process is initiated with the `ping` command.

Have the students do an exercise on the ping procedure. Discuss the use of the DNS function. Explain that the DNS must be available to use a domain name instead of an IP address when the `ping` command is used. Also point out that a way to check the function of DNS is to ping the same destination by domain name and by IP address. If the remote location responds to the IP address but not to the domain name then this indicates a DNS issue. Explain that a location may be unreachable because of security restrictions. ICMP may be a blocked protocol.

### 8.1.6 Detecting excessively long routes

Situations in a network can occur where datagrams travel in a circle and never reach their destination. This could occur because no path exists between a source and a destination that conforms to the requirements of the routing protocol. This could be caused by incorrect routing information. Explain that paths with too many hops and circular paths create an excessively long route. The packet will eventually reach the end of its life, known as time to live (TTL). The TTL is not related to the hop count value of RIP. RIP advertisements are broadcast. That means they will not go farther than the local segment. The reachability of RIP is controlled by the routing protocol. It maintains a hop count metric that cannot exceed 15. This means that a route will not be advertised further than 15 hops. It does not mean that packets cannot travel more than 15 hops. The process is as follows:

1. As each router processes the datagram, the TTL value decreases by one.
2. When the TTL value reaches zero, the packet is discarded.



### 8.1.7 Echo messages

ICMP message formats have three fields:

- Type
- Code
- Checksum

The type field indicates the type of ICMP message that is sent. The code field includes additional information that is specific to the message type. The checksum field is used to verify the integrity of the data. Create an example to help students understand this format. This is an important concept to help the student understand causes of ICMP "destination unreachable" messages.

### 8.1.8 Destination unreachable message

Hardware failures, improper protocol configuration, disabled interfaces, and incorrect routing information are some of the reasons for unsuccessful delivery of data. Give the students examples similar to the figures in the curriculum. Specify values and indicate the reason for each failure. Explain that the students must understand the various causes of ICMP "destination unreachable" messages to effectively troubleshoot an IP network.

### 8.1.9 Miscellaneous error reporting

Devices that process datagrams may not be able to forward a datagram due to some type of error in the header. The error does not relate to the state of the destination host or network, but it will still prevent the datagram from being processed and delivered.

## 8.2 TCP/IP Suite Control Messages

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** None

**Optional TIs:** All

**Course Level Claim:** Students can describe the operation of ICMP and identify the reasons, types, and format of associated error and control messages.

**Hands-on skills:** none

### 8.2.1 Introduction to control messages

ICMP is an integral part of the TCP/IP protocol suite. All IP implementations must include ICMP support for the following reasons:

- Since IP does not guarantee delivery, it has no method to inform hosts when errors occur.
- IP has no built-in method to provide information or control messages to hosts.
- ICMP is necessary to perform these functions for IP.

Explain to the students that unlike error messages, control messages are not the result of lost packets or error conditions. Instead, they are used to inform hosts of conditions such as network congestion or the existence of a better gateway to a remote network. Like all ICMP messages, ICMP control messages are encapsulated.

### 8.2.2 ICMP redirect/change requests

An ICMP redirect/change request can only be initiated by a gateway, which is commonly used to describe a router. All hosts that communicate with multiple IP networks must be configured with a default gateway. This default gateway is the address of a router port connected to the same network as the host. Normally there is a single gateway. In some circumstances a host can connect to a segment that has two or more directly connected routers. In these situations, the default gateway may need to use a redirect/change request to inform the host of the best path. Explain this concept with the students and make sure they understand this important process.

Default gateways only send ICMP redirect/change requests if the following conditions are met:

- The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
- The subnet/network of the source IP address is the same subnet/network of the next hop IP address of the routed packet.
- The datagram is not source-routed.

- The route for the redirect is not another ICMP redirect or a default route.
- The router is configured to send redirects.

Make sure students understand default gateways. Instruct students to look at the router lab setup and visually determine the default gateway of the host attached to it.

### 8.2.3 Clock synchronization and transit time estimation

Networks that connect to each other over vast distances choose their own method of clock synchronization. As a result, hosts on disparate networks who attempt to communicate with software that requires time synchronization can encounter problems. The ICMP timestamp message type is designed to help alleviate this problem.

The ICMP timestamp request message allows a host to ask the remote host for the current time. The remote host uses an ICMP timestamp reply message to respond to the request. The type field on an ICMP timestamp message can be either a 13 or 14 timestamp reply. The code field value is always set to zero. The ICMP timestamp request contains an originate timestamp, which is the time on the requesting host just before the timestamp request is sent. The receive timestamp is the time that the destination host receives the ICMP timestamp request. The transit timestamp is filled in just before the ICMP timestamp reply is returned. Originate, receive, and transit timestamps are computed in numbers milliseconds elapsed since midnight (00:00), Universal Time.

The host that originated the ICMP timestamp request can use these timestamps to estimate transit time across the network. The host can subtract the originate time from the transit time to guess the transit time. However this can vary widely based on traffic and congestion. The host that originated the ICMP timestamp request can also estimate the local time of the remote computer. This is an important concept for the students to understand. Make sure that they also understand that NTP, which is a UDP protocol, is used to maintain the time between systems.

### 8.2.4 Information requests and reply message formats

ICMP information requests and reply messages were originally intended to allow a host to determine the number of the network it resided on. However, BOOTP and DHCP are now used to allow hosts to obtain the network number to which they are attached.

### 8.2.5 Address mask requests

A subnet mask is important to identify network, subnet, and host bits in an IP address. If a host does not know the subnet mask, it may send an address mask request to the local router. The router responds with an ICMP address mask reply. If the address of the router is known, this request may be sent unicast. If the address is not known, the request will be a broadcast. When the router receives the request, it will respond with an address mask reply. This reply will identify the correct subnet mask. This is an important concept for the students to understand. This is also a good time to review IP addressing.

### 8.2.6 Router discovery message

When a host on a network boots and has not been manually configured with a default gateway, it can learn the available routers through the process of router discovery. This

process begins when the host sends a multicast router solicitation message to all routers with the address 224.0.0.2. If a router solicitation message is sent to a router that does not support the discovery process, the solicitation will go unanswered. However, if it is supported, a router advertisement is sent in return.

### 8.2.7 Router solicitation message

A host will generate an ICMP router solicitation message in response to a missing default gateway. This message is sent multicast. This is the first step in the router discovery process. A local router will respond with a router advertisement that identifies the default gateway for the local host.

### 8.2.8 Congestion and flow control messages

Congestion occurs when multiple computers try to access the same receiver or when traffic from a high speed LAN reaches a slower WAN connection. The effect of congestion on a network is dropped packets that result in a loss of data. To reduce data lost, ICMP messages must be sent to the source of the congestion. This type of ICMP message is called a source-quench message. The source-quench message notifies the sender of the congestion and asks the sender to reduce its rate. This usually reduces the congestion. The rate of transmission will slowly increase if no other source-quench messages are received. One way ICMP source-quench messages might be used effectively is in a SOHO. Develop an example of network congestion. Have the students come up with their own ideas about the factors that cause network congestion.

## Module 8 Summary

Before students begin Module 9, they should know where to look for many of the error messages they may encounter.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 8 exam. This is a very descriptive module so vocabulary or scenario-based quizzes may be the preferred form of assessment.

Students should understand the following main points:

- IP is a best-effort delivery method that uses ICMP messages to alert the sender that the data did not reach its destination.
- ICMP echo request and echo reply messages allow the network administrator to test IP connectivity to aid in the troubleshooting process.
- ICMP messages are transmitted with the IP protocol so their delivery is unreliable.
- ICMP packets have their own special header information, which starts with a type field and a code field.
- Potential causes of specific ICMP error messages
- The functions of ICMP control messages
- ICMP redirect/change request messages
- ICMP clock synchronization and transit time estimation messages
- ICMP information request and reply messages
- ICMP address mask request and reply messages
- ICMP router discovery message
- ICMP router solicitation message
- ICMP congestion and flow control messages

# Module 9: Basic Router Troubleshooting

## Overview

When teaching Module 9, emphasize the fact that the ability to interpret a routing table is of fundamental importance to networking professionals. This module is dedicated to routing tables and troubleshooting tools such as the `show ip route` command.

### Module 9 Caution

Students need to understand how to use these commands and interpret their output. This module is usually very interesting to students.

Students who complete this module should be able to perform the following tasks:

- Use the `show ip route` command to gather detailed information about the routes installed on the router
- Configure a default route or default network
- Understand how a router uses Layer 2 and Layer 3 addressing to move data through the network
- Use the `ping` command to perform basic network connectivity tests
- Use the `telnet` command to verify the application layer software between source and destination stations
- Troubleshoot by sequential testing of OSI layers
- Use the `show interfaces` command to confirm Layer 1 and Layer 2 problems
- Use the `show ip route` and `show ip protocol` commands to identify routing issues
- Use the `show cdp` command to verify Layer 2 connectivity
- Use the `traceroute` command to identify the path packets take between networks
- Use the `show controllers serial` command to ensure the proper cable is attached
- Use basic `debug` commands to monitor router activity

## 9.1 Examining the Routing Table

**Essential Labs:** 9.1.1, 9.1.2, and 9.1.8

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can configure, verify, analyze, and troubleshoot simple distance vector routing protocols.

**Certification-Level Claim:** Students can troubleshoot and configure routing protocols based on user requirements.

**Hands-on skills:** none

### 9.1.1 The show ip route command

One of the primary functions of a router is to determine the best path to a given destination. A router learns paths from the configuration or from other routers through routing protocols. They use RAM to store this routing information in routing tables. A routing table contains the best available routes to destinations. The `show ip route` command displays the contents of the IP routing table. The routing table contains entries for all known networks and subnetworks and a code that indicates how that information was learned. Discuss how valuable the `show ip route` command is to network troubleshooting.

Routes can be added to a router through two methods:

- **Static routing** – An administrator manually defines routes. These routes do not change until a network administrator manually programs the changes.
- **Dynamic routing** – Routers follows rules defined by a routing protocol to exchange routing information. These routes change automatically as neighboring routers update each other with new information.

Discuss with the students the differences between static routing and dynamic routing. This is an important concept for the students to understand. The instructor should also emphasize that the router would not know what to do with a packet if there was no route to forward it toward the destination.

### 9.1.2 Determining the gateway of last resort

Routers do not maintain routes to every possible destination. Instead, routers can keep a default route, or a gateway of last resort. The router will use this default route to forward a packet to a different router. Default routes can be statically entered by an administrator or dynamically learned through a routing protocol. Before routers can dynamically exchange information, an administrator must configure at least one router with a default route.

An administrator can use two different commands to configure default routes:

- **ip route 0.0.0.0 0.0.0.0** [next-hop-ip-address | exit-interface]
- ip default-network

The **ip default-network** command establishes a default route in networks with dynamic routing protocols. Discuss the important concept of the gateway of last resort and the two commands used to configure default routes. Have the students brainstorm and present their ideas on why routers do not maintain routes to every possible destination to the class. One thing the students should know is that the **ip route 0.0.0.0 0.0.0.0** command is referred to as the “quad zero route”.

### 9.1.3 Determining route source and destination

Path determination occurs at the network layer, which is Layer 3. The path determination function enables a router to evaluate the available paths to a destination and to establish the preferred way to handle a packet. The network layer provides best-effort, end-to-end packet delivery. The network layer uses the IP routing table to send packets from the source network to the destination network. Discuss Layer 3 of the OSI model as a review. This should be a concept that the students have already mastered.

### 9.1.4 Determining L2 and L3 addresses

While network layer addresses are used to get packets from their source to destination, it is important to understand that a different type of address is used to get packets from one router to the next. For a packet to get from the source to the destination, both Layer 2 and Layer 3 addresses are used. Explain how important this concept is for the students to understand. The Layer 3 address is used to route a packet from the source network to the destination network. The source and destination IP addresses remain the same. The MAC address changes at each hop or router. A data link layer address is necessary because the source host must have a way to address the next-hop router to which the packets are being forwarded.

For students to understand the routing process, the Layer 2 and 3 addresses must be understood. Be sure to review the various names for IP addresses, such as a Layer 3 address, a network layer address, or a logical address. Review the same concept for a MAC address, that it is also called a Layer 2 address, a data link address, or a physical address. It is also important to understand that the MAC will change while the IP will remain the same. Remind the students that the packet will remain intact from the source host to destination host. At each hop along the path a new frame is created and addressed in the frame to the next hop.

### 9.1.5 Determining route administrative distance

One of the most intriguing aspects of Cisco routers is how the router chooses which route is the best. As each routing process receives updates and other information, it chooses the best path to any given destination and attempts to add this path to the routing table. The router decides whether or not to add the routes presented by the routing processes based on the administrative distance of each route. The route with the lowest administrative distance is considered the best route.



Explain administrative distances to the students. The administrative distance represents the trustworthiness of the source of a route. The Cisco IOS is designed to trust directly connected routes more than any other source. Directly connected routes have the lowest administrative distance of zero. The IOS also trusts routes that are configured by a network administrator, which are static routes. These have an administrative distance of one. Students should also learn the administrative distances of RIP, IGRP, EIGRP, and OSPF. The administrative distance must not be confused with routing metrics. Metrics are calculated and compared among routes from the most trusted routing source. The router will select the route from the best administrative source with the lowest metric. This is an important concept for the students to understand.

### 9.1.6 Determining the route metric

Routing protocols use metrics to determine the best route to a destination. The metric is a value that measures the desirability of a route. Some routing protocols use only one factor to calculate a metric. For example, RIP only uses hop count as a metric. Other protocols base their metric on bandwidth, delay, load, reliability, ticks, maximum transmission unit, and cost. Discuss with the students the differences between each of these metrics so they fully understand what is used to calculate the best route.

Each routing algorithm interprets what is best in its own way. The algorithm generates a number, called the metric value, for each path through the network. The smaller the metric value is, the better the path. Review the administrative distances covered in an earlier section. Make sure students understand the difference between administrative distances and metrics. Also explain that routes from different protocols cannot be compared since routing protocols use different metrics and different methods to determine the metric value.

### 9.1.7 Determining the route next hop

Routing algorithms fill routing tables with information. Destination or next hop associations tell a router that a particular destination can be reached if the packet is sent to a particular router that represents the next hop on the way to the final destination. Have students look at routing table examples and determine the next-hop router for a network.

### 9.1.8 Determining the last routing update

A network administrator can use the following commands to find the last route update:

- show ip route
- show ip route *network*
- show ip protocols
- show ip rip database

Stress the importance of these commands. Use examples to show the students the information generated by these commands.

### 9.1.9 Observing multiple paths to destination

Some routing protocols support multiple paths to the same destination. Multipath algorithms permit traffic over multiple lines, provide better throughput, and are more reliable. Discuss with the students their ideas on why it would be better to have multiple paths through the network. Discuss redundancy and reasons why all networks are not redundant.

## 9.2 Network Testing

**Essential Labs:** 9.2.6

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can use embedded Layer 3 through Layer 7 protocols to establish, test, suspend, or disconnect connectivity to remote devices from the router console.

**Certification Level Claim:** Students can describe network communications in layered models, perform simple LAN troubleshooting, and use the OSI model as a guide for systematic network troubleshooting.

**Hands-on skills:** none

### 9.2.1 Introduction to network testing

Basic testing of a network should move through each layer of the OSI reference model. Begin with Layer 1 and work to Layer 7 if necessary. Instruct the students to look for simple solutions first when they test a network. Some of the most common problems on IP network result from errors in the addressing scheme. Reinforce how important IP addressing schemes are to a network. Explain to students that a large part of their role in the workplace will require troubleshooting.

### 9.2.2 Using a structured approach to troubleshooting

Troubleshooting is a process that allows a user to find problems in a network. There should be a structured or orderly process to troubleshooting based on the networking standards defined by an administration. Documentation is a very important part of the troubleshooting process.

Emphasize to the students that documentation is important, but probably the least performed task in network management. Have the students brainstorm ideas about why a structured approach is important to troubleshooting. Discuss the ideas with the class.

Emphasize the two structured approaches explained in the curriculum. Since these are not the only two approaches, instruct the students to work in groups and develop their own structured approaches to troubleshooting. The students need to understand that the troubleshooting process can create additional problems. To prevent this, make sure students know that they should reverse any processes they use to solve the issue. Failure to do so can add to the network problems.

### 9.2.3 Testing by OSI layers

Testing should begin with Layer 1 of the OSI model and work to Layer 7 if necessary. The `ping` command is used at Layer 3. The `telnet` command is used at Layer 7. Both of these commands will be discussed in detail in a later section. It is important for the students to understand which types of errors occur at the different layers of the OSI model. This is a good opportunity to group students together to practice for an exam or earn extra credit through competitive activities. For example, describe a type of error and have the teams compete to determine the associated layer.

Relevant TIs from CCNA 2 v2.1.4 are 13.1.1 and 13.1.5.

The students need to understand the ping process and what is tested by each ping:

- ping the loopback address
- ping the interface address
- ping the local router interface address
- ping a remote host address

### 9.2.4 Layer 1 troubleshooting using indicators

Indicator lights are useful troubleshooting tools. Most interfaces or NICs have indicator lights that show if there is a valid connection. The interface may also have lights to indicate if traffic is being sent or received. Have the students discuss possible Layer 1 problems. Instruct students to check for the simplest of problems first such as power cords or electricity.

### 9.2.5 Layer 3 troubleshooting using ping

The ping utility is used to test network connectivity. Echo protocols are used to test if protocol packets are being routed. The `ping` command sends a packet to the destination host and then waits for a reply packet from that host. Results from this echo protocol can help evaluate the path-to-host reliability, delays over the path, and if the host can be reached or is functional. The `ping` command can be invoked from both user EXEC mode and privileged EXEC mode. To use the extended `ping` command, the user must be in privileged EXEC mode. Explain to the students that it is a good idea to use the `ping` command when the network functions properly to see how the command works under normal conditions. This can also be used to make comparisons when troubleshooting. The students should relate ping to reachability.

### 9.2.6 Layer 7 troubleshooting using Telnet

Telnet is a virtual terminal protocol that is part of the TCP/IP protocol suite. Telnet allows the verification between source and destination stations. The `telnet` command provides a virtual terminal so administrators can use Telnet operations to connect with other routers that use TCP/IP. The `telnet` command will be discussed in later sections of the curriculum. At this point, students should understand the functions of Telnet.

## 9.3 Troubleshooting Router Issues Overview

**Essential Labs:** 9.3.4, 9.3.5, and 9.3.7

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can use the commands incorporated within IOS to analyze and rectify network problems.

**Certification-Level Claim:** Students can perform simple WAN troubleshooting.

**Hands-on skills:** none

### 9.3.1 Troubleshooting Layer 1 using `show interfaces`

The Cisco IOS contains many troubleshooting commands. The `show` commands are widely used. The `show interfaces` command is used to check the status and statistics of the interfaces. The `show interfaces serial` command displays the line and data link protocol status. It also provides information to help diagnose other Layer 1 issues that are not as easy to determine. These problems include line interruptions, faulty switch, faulty DSU, or faulty router hardware. Have the students view the results displayed by these commands and discuss the results to make sure they understand the output. This is an important concept and valuable tool for troubleshooting.

### 9.3.2 Troubleshooting Layer 2 using the `show interfaces`

The `show interfaces` command is possibly the most important tool to discover Layer 1 and Layer 2 problems in the router. The first parameter refers to the physical layer. The second parameter indicates if the IOS processes that control the line protocol consider the interface to be usable. This is determined by whether keepalives are successfully received. If the interface misses three consecutive keepalives, the line protocol is marked as down. The `show interfaces serial` command should be used after a serial interface is configured to verify the changes and that the interface is operational.

View these results with the students and discuss the results to make sure they understand the output. This is an important concept and valuable tool for troubleshooting. The students are not expected to understand all the fields contained in the `show interfaces` command output. This command will be revisited in CCNA 4 and more information will be presented.

### 9.3.3 Troubleshooting using `show cdp`

CDP advertises device information to its direct neighbors that includes MAC and IP addresses and outgoing interfaces. The output from the `show cdp neighbors` command displays information about directly connected neighbors. This information can be used to debug connectivity issues. The `show cdp neighbor detail` command returns specific device details such as the active interfaces, the port ID, and the device. The version of Cisco IOS that is used on the remote devices is also shown.

This is an important concept for the students to understand to help in the troubleshooting process.

Two important facts for the students to learn are that CDP is Cisco proprietary, which means that it only works between Cisco devices, and that CDP only works between directly connected devices.

### 9.3.4 Troubleshooting using traceroute

The **traceroute** command is used to discover the routes that packets take when they travel to their destination. The **traceroute** command can also be used to test the network layer on a hop-by-hop basis.

The **traceroute** command output shows a list of hops that the traceroute successfully reaches. Traceroute output can also be used to indicate the specific hop at which the failure occurs. Traceroute also provides output that indicates the relative performance of the links. There must be routes in both directions for the **traceroute** or **ping** data to successfully make a round trip between routers. This is an important concept for the students to understand to help in the troubleshooting process. Help students associate **traceroute** with determining actual path.

### 9.3.5 Troubleshooting routing issues

The **show ip route** command is perhaps the most important command for troubleshooting routing issues. This displays the contents of the IP routing table. The output shows the entries for all known networks and subnetworks and how that information was learned.

If the output of the **show ip route** command does not show the expected learned routes, then it is possible that routing information is not being exchanged. In this case, use the **show ip protocols** command on the router to check for a possible misconfigured routing protocol.

The **show ip protocols** command output can be used to diagnose a multitude of routing issues. It can be used to identify a router that is the source of incorrect router information. This is an important concept for the students to understand to help in the troubleshooting process. In the output of the **show ip route** command, clarify the values that represent the administrative distance, metric, next hop interface, and the update time. In the **show protocols** output, clarify the values that represent the update timers, the networks being routed, and the routing sources.

### 9.3.6 Troubleshooting using show controllers

The **show controller serial** command can be used to identify the type of cable that is connected to the routers without inspecting the cables. This can be used to find a serial interface with no cable, the wrong type of cable, or a defective cable.

The **show controller serial** command queries the integrated circuit chip that controls the serial interface and displays information about the physical interface. It also produces a tremendous amount of output, which includes the cable type. Most of the output is internal technical details about the controller chip status. This information requires specific knowledge of the integrated circuit. This is an important concept for the students to understand to help in

the troubleshooting process. Students need to realize that there is a lot of output that will be completely unfamiliar to them. The two main reasons for them to use this command are to discover the cable type connected to the serial interface and to see the clock rate on the interface with the DCE cable.

### 9.3.7 Introduction to debug

The **debug** command is used to display dynamic data and events. The **debug** command output gives more insight into the current events of the router. The dynamic output of the **debug** command has a high performance cost. It produces a high processor overhead that disrupts normal router operation. Debug should be used conservatively. Stress to the students that debug is a very important tool. However, this command can disrupt router operations and cause network performance to decrease drastically. It should only be used to diagnose a problem and then it should be turned off.

## Module 9 Summary

Before students begin Module 10, they must be able to read and interpret a routing table and must have mastered a range of IOS commands for troubleshooting.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 9 exam. Paper activities and hands-on router challenges should be used to give students troubleshooting practice. Consider giving students previously-bugged configuration files so they can demonstrate their troubleshooting skills in a timed, controlled setting.

Students should understand the following main points:

- Use and understand the output of the **show ip route** command
- Determine the gateway of last resort
- Determine the route source and destination address
- Determine the route administrative distance
- Determine the route metric
- Determine the route next hop
- Determine the last route update
- Observe multiple paths to a destination
- Use a structured approach to troubleshooting
- Test by OSI layers
- Use indicators to troubleshoot Layer 1
- Use the **ping** command to troubleshoot Layer 3
- Use the **telnet** command to troubleshoot Layer 7
- Use the **show interfaces** command to troubleshoot Layer 1 and Layer 2
- Use the **show ip route** and **show ip protocols** commands to troubleshoot routing issues
- Use the following commands to troubleshoot various router problems:
  - **show cdp**
  - **tracert**
  - **show controllers serial**
  - **debug**

# Module 10: Intermediate TCP/IP

## Overview

Module 10 is a good place to have the student compare IP and TCP. It is essential for the students to understand that IP is connectionless and unreliable, while TCP is connection-oriented and reliable. In this section, the students will gain an understanding of the transport layer ports that allows for the full communications process between two hosts. The following objectives will be covered:

- Multiple conversations between hosts
- Ports used for services and clients
- Port numbering and well known ports
- Comparison of MAC addresses, IP addresses, and ports

Consider the use of network analysis or protocol sniffing software such as Fluke Protocol Inspector to analyze the operation of TCP on live networks.

### Module 10 Caution

TCP was introduced in CCNA 1 but there is much more detail in this section. Students need to understand TCP. TCP ports and sessions are the foundations of network performance, control, and security. This is very challenging material for students who are still trying to separate the functions of Layer 2 headers, Layer 3 headers, and Layer 4 headers. The numbering of bytes in the back-and-forth exchange of SYN and ACK in TCP is difficult to understand. Work out examples for students.

Students who complete this module should be able to perform the following tasks:

- Describe TCP and its functions
- Describe TCP synchronization and flow control
- Describe UDP operation and processes
- Identify common port numbers
- Describe multiple conversations between hosts
- Identify ports used for services and clients
- Describe port numbering and well known ports
- Understand the differences and the relationship between MAC addresses, IP addresses, and port numbers



## 10.1 TCP Operation

**Essential Labs:** 10.1.6

**Optional Labs:** None

**Core TIs:** 10.1.6

**Optional TIs:** 10.1.1 – 10.1.5, and 10.1.7

**Course-Level Claim:** Students can describe the operation of the major transport layer protocols and the interaction and transportation of application layer data.

**Certification-Level Claim:** Students can evaluate the TCP/IP communication process and its associated protocols.

**Hands-on skills:** none

### 10.1.1 TCP operation

IP addresses allow for the routing of packets within and between networks. However, it makes no guarantee about delivery. The transport layer is responsible for the reliability of data flow. This is accomplished through the use of sliding windows and sequencing numbers along with a synchronization process that ensures communication. Have the students come up with an analogy. One excellent example is a student who studies a foreign language for one year, visits the country where the language is used, and asks everyone to repeat their words for reliability and speak slowly for flow control.

### 10.1.2 Synchronization or three-way handshake

TCP is connection-oriented. Prior to data transmission two hosts go through a synchronization process to establish a virtual connection. This process ensures that both sides are ready for data and allows for the devices to determine the initial sequence numbers. This process is a three-way handshake. Sequence numbers (SYN) and the role they play will be discussed in detail in a later section. At this point it is important for students to understand that sequence numbers are used to initiate communication between two devices. The sequence numbers give each host a way to acknowledge the SYN bits so that the receiver knows the sender responds to the proper connection request. This is done with bits in the TCP header. These bits are called flags. The two flags involved are Sequence numbers (SYN) and Acknowledge numbers (ACK). These flags are used to synchronize the SYN and ACK numbers between the hosts. This will initialize the new session.

The three-way handshake is a three-step process that establishes the virtual connection between two devices:

1. The source host initiates a connection. The host sends a packet with the SYN bit set and indicates an initial sequence number of  $x$  with a bit in the header set to indicate a connection request.
2. The destination host receives the packet, records the sequence number of  $x$ , replies with an acknowledgment of  $x + 1$ , and includes its own initial sequence number of  $y$ . It also sets the SYN bit to indicate the start of the return conversation.

3. The source host responds with a simple acknowledgement of  $y + 1$  to indicate that it received the previous ACK. This finalizes the connection process.

The three-way handshake is an important concept for the student to understand. A relevant TI from CCNA 2 v2.1.4 is 9.1.6.

### 10.1.3 Denial of service attacks

Denial of service (DoS) attacks are designed to deny services to legitimate hosts that attempt to establish connections. DoS attacks are commonly used by hackers to halt system responses. One example is SYN flooding, which occurs during the three-way handshake process. As a packet with the SYN bit set is sent, it includes its IP address and the destination IP address. This information is then used by the destination host to send the SYN/ACK packet back. In the DoS attack, the hacker initiates a synchronization but spoofs the source IP address. The destination device responds to a non-existent, unreachable IP address and is placed in a waiting state. This waiting state is placed in a holding area that uses memory. Hackers flood the host with these false SYN requests to deplete all the connection and memory resources of the host. To defend against these attacks, system administrators may decrease the connection timeout period and increase the connection queue size. This is an important concept for the students to understand to help prevent hackers from creating chaos in a network.

### 10.1.4 Windowing and window size

Data is often too large to be sent in a single data segment. TCP breaks data into segments. A good analogy is small children who cannot eat large pieces of food. Their food must be cut into smaller pieces to be eaten. Another way to explain the advantages of this segmentation is to ask the students to imagine a 200-MB file that needs to be transferred. Ask students the following questions:

- What if networking did not allow the file to be segmented?
- How long would the other hosts on the network have to wait to get any network access?

Even without an exact answer the students can see the inefficiency of streaming on all the other hosts. Calculate the wait with the formula  $(200\text{MB} \times 8\text{bits/byte})/\text{media speed}$ .

After data is segmented, it must be transmitted to a destination device. Flow control regulates how much data is sent during a transmission. The process of flow control is known as windowing. Window size determines how much data can be transmitted at one time. The host must receive an ACK before any more data can be sent. TCP uses sliding windows to determine transmission size. This allows for negotiation of the window size to allow for more than one byte to be sent. This allows for the destination device to tell the source to decrease or increase the amount of data being sent. This is an important concept for the students to understand. This helps the student understand the entire process of TCP and why it is considered reliable and connection-oriented.

### 10.1.5 Sequencing numbers

Since TCP breaks data into segments, the receiver must reassemble the data segments once all of the data is received. TCP issues a sequence to the data segments so that the receiver can properly reassemble the bytes into their original form. Emphasize that this is important because data may arrive out of order to the destination. The sequence numbers indicate the correct order in which to put the bytes back together. Also mention that UDP does not use sequencing numbers. Sequencing numbers also act as reference numbers so that the receiver knows if it has received all of the data and can identify any missing pieces so the sender can retransmit them. Explain that this offers increased efficiency since the sender only needs to retransmit the missing segments.

### 10.1.6 Positive acknowledgements

A common step in sliding windows, synchronization, and data sequencing is acknowledgment. An acknowledgment field follows the sequence number field. TCP uses acknowledgement and retransmission to control data flow and confirm data delivery. This is a good time to stress the main difference between IP and TCP. IP has no verification method to determine that data has reached its destination. Positive acknowledgment and retransmission (PAR) is a common technique that is used to provide reliability. With PAR, the source sends a packet, starts a timer, and waits for an ACK before the next packet is sent. If the timer expires, the source retransmits the packet and starts the timer again. TCP uses expectational acknowledgments, in which the acknowledgement number refers to next octet that is expected. Windowing is also a flow-control mechanism. If there is a window size of three, the source can send three octets to the destination. It then waits for an acknowledgment. When it is received, another three octets are sent. If the data is not received due to overflowing buffers, no acknowledgment is sent. Therefore, it is known that the data must be retransmitted and the transmission rate should be slowed.

To slow the transmission rate, the window size can be reduced. The transmitting host will transmit a smaller amount and wait on the acknowledgement before transmitting more segments. Make sure the students understand the differences between these processes. This will help them understand the entire TCP process. One final but very important concept is that sequencing and acknowledgement numbers are handled on a session-by-session basis. Each session between hosts uses its own unique set of sequencing and acknowledgement numbers.

### 10.1.7 UDP operation

The TCP/IP protocol stack contains many different protocols. Some are:

- **IP** – provides connectionless unreliable transmission at Layer 3
- **TCP** – provides connection-oriented reliable transmission at Layer 4
- **UDP** – provides connectionless unreliable transmission at Layer 4

Both TCP and UDP use IP as their underlying protocol. TCP must be used when applications need to guarantee the delivery of a packet. When applications do not need a guarantee, UDP is used. It is a faster, connectionless delivery mechanism. Stress to the students that UDP does not use windowing or acknowledgments and does not require sequencing numbers. Application layer protocols provide more reliability. Since the UDP header is smaller than the TCP header, UDP has less overhead.

UDP is often used for applications and services such as real-time audio and video. These applications require less overhead. They also do not need to be resequenced since packets that arrive late or out of order have no value.

## 10.2 Overview of Transport Layer Ports

**Essential Labs:** 10.2.5

**Optional Labs:** None

**Core TIs:** 10.2.5

**Optional TIs:** 10.2.1 – 10.2.4, and 10.2.6

**Course-Level Claim:** Students can describe the operation of the major transport layer protocols and the interaction and transportation of application layer data.

**Certification-Level Claim:** Students can evaluate TCP/IP communication process and the associated protocols.

**Hands-on skills:** none

### 10.2.1 Multiple conversations between hosts

At any given moment, thousands of packets destined for hundreds of different services travel through a network. Servers provide services for a multitude of different requests. This causes unique problems for addressing of packets. For example, if a server uses SMTP and WWW services, a client cannot construct a packet that is destined for just the IP address of the server with TCP because both SMTP and WWW use TCP as their transport layer protocol. A port number must be associated with the conversation to ensure that the packet reaches the appropriate service.

Port numbers are used to keep track of different conversations that cross the network at the same time. Port numbers are needed when a host communicates with a server that uses multiple services. Both TCP and UDP use port numbers to pass information to the upper layers. Software developers use the well-known port numbers defined in RFC1700. Conversations that do not involve applications with well-known port numbers are assigned port numbers that have been randomly selected from a specific range.

Port numbers have the following ranges:

- Numbers below 255 are used for public applications
- Numbers from 255-1023 are assigned to marketable applications
- Numbers above 1023 are unregulated

A good analogy to help students understand this process is a post office box number. Each piece of mail is sent to a zip code, city, and then a P. O. Box. Similarly, the IP address and transport layer send the packet to the correct server, but the port number guarantees that the packet will contact the correct application.

## 10.2.2 Ports for services

Services that are used on hosts must have a port numbers assigned so communication can occur. Some ports are reserved in both TCP and UDP. These are considered well-known ports. Students must know these port numbers. Explain to the student that a question mark (?) can be used in the router to display the port numbers. However, students must learn the most common port numbers. These ports and their activities can be examined on a workstation from the command prompt with the `netstat -a` command. The ports that are listed as listening are services.

A good way to explain this concept is a server service listens on a given port number. A client will initiate a session with the server by addressing that particular port number. All inbound segments have a destination port number. An application layer protocol or service looks at this port number to see if its port number is being addressed. If it is not, then the service ignores the segment. Emphasize that the client initiates the session. The server is listening and will respond when addressed.

## 10.2.3 Ports for clients

When a client connects to a service on a server, a source and destination port must be specified. Source ports, which are set by the client, are determined dynamically. A client usually determines the source port by randomly assigning a number above 1023. Clients and servers use ports to distinguish what process each segment is associated with. This is an important concept for the students to understand about port numbers. Explain that the server responds with the same port numbers except the source and destination port numbers are swapped. For example, if the client initiates a session with a source port number of 1094 and a destination port number of 23, then the server will respond with a source port number of 23 and a destination port number of 1094.

## 10.2.4 Port numbering and well known port numbers

Port numbers are represented by two bytes in the header of a TCP or UDP segment. This 16-bit value can result in port numbers that range from 0 to 65535. Port numbers are divided into three different categories:

- Well known ports
- Registered ports
- Dynamic or private ports

The first 1023 are well known ports. Registered ports range from 1024 to 49151. Ports between 49152 and 65535 are dynamic or private ports. Discuss the differences between these ports with the students. Also, let the students know that services can use the upper port numbers. This can be done for private applications or for security. An example of using a private port for security is running a Telnet server listening to port 14002, instead of the well-known port 23. Since the port is not the standard port 23, the open port 14002 would have to be known or discovered by a user to successfully telnet to this host.

## 10.2.5 Example of multiple sessions between hosts

Port numbers are used to track multiple sessions that occur between hosts. The port number combined with the network address forms a socket. A pair of sockets, one for the source and one for the destination, forms a unique connection. For example, a host could have a Telnet connection on port 23 and surf the net on port 80 at the same time. Explain to the students that port numbers must be different because they represent different protocols and different sockets. Emphasize the fact that sequencing and acknowledgement numbers are handled on a session-by-session basis. Each session between hosts uses its own unique set of sequencing and acknowledgement numbers.

## 10.2.6 Comparison of MAC addresses, IP addresses, and port numbers

Port numbers are located at the transport layer and are serviced by the network layer. The IP address is assigned at the network layer and is serviced by the data link layer that assigns the MAC address.

A good analogy is a letter. The address on a letter consists of a name, street, city, and state. These can be compared to the port, MAC, and IP address used for network data. The name on the envelope would be the same as the port number, the street address would be the MAC address, and the city and state would be the IP address. Multiple letters can be mailed to the same MAC and IP address, but different port numbers would be different family members living in the same household.

To better explain this, the instructor may want to ask some questions and start a discussion:

- Could a protocol be routable with only Layer 3 addressing? No. A new frame is built as the packet is transmitted from the router interface. The Layer 2 address is used for the delivery of data within the local segment. If only Layer 2 addressing is used then the data can only be delivered locally. If a router cannot find a Layer 3 address after the frame is discarded, it will not know what to do with the packet.
- Could there be multiple sessions between the same hosts without port numbers? No. Port numbers distinguish the various conversations between hosts. Without port numbers, there would be no way for the hosts to determine to which session a packet belongs.
- What is an option if there is no Layer 2 address? Broadcast all the frames. Generally, this is not an acceptable solution. When a frame is broadcast, every host in the network segment will examine the packet to see if it is addressed to that host. This forces the host to use an interrupt to notify the CPU. The host must stop what it is doing and service this interrupt. This type of broadcast communication is an inefficient use of bandwidth and also wastes valuable CPU resources on the hosts.

## Module 10 Summary

Before students begin Module 11, they must be able to compare and contrast the roles of MAC addresses, IP addresses, and port numbers.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 10 exam.

Students should understand the following main points:

- TCP operation description
- Synchronization process or three-way handshake
- Denial-of-service attacks
- Windowing and window size
- Sequencing numbers
- Positive acknowledgement and retransmission (PAR)
- UDP operation
- Multiple conversations between hosts
- Ports for services
- Ports for clients
- Port numbering and well-known ports
- Example of multiple sessions between hosts
- Comparison of MAC addresses, IP addresses, and port numbers

# Module 11: Access Control List (ACLs)

## Overview

When teaching Module 11, emphasize the importance of access control lists (ACLs). Network administrators must establish a way to deny unwanted access to a network and allow internal users to access necessary services. Security tools such as passwords, callback equipment, and physical security devices are helpful. However, they often lack the flexibility of basic traffic filtering and the controls most administrators prefer. ACLs will be used for many aspects of networking. These include security, dial on demand routing, and all types of route filtering techniques. Quality of Service routers provide basic traffic filtering capabilities such as the use of ACLs to block Internet traffic. An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols.

**Module Caution:** It may be difficult for students to understand the concept of ACLs. This topic will require additional time for students to understand. Work through numerous examples. Have students finish the hands-on labs and e-Labs. Consider spending less time on Modules 1, 5, 8, and 10 to make sure ACLs are properly learned.

Students who complete this module should be able to perform the following tasks:

- Describe the differences between standard and extended ACLs
- Explain the rules for placement of ACLs
- Create and apply named ACLs
- Describe the function of firewalls
- Use ACLs to restrict virtual terminal access

## 11.1 Access Control List Fundamentals

**Essential Labs:** None

**Optional Labs:** None

**Core TIs:** All

**Optional TIs:** none

**Course-Level Claim:** Students can identify the application of packet control with various access control lists.

**Certification-Level Claim:** Students can implement access lists, develop an access list to meet user specifications, and evaluate rules for packet control.

**Hands-on skills:** none



## 11.1.1 Introduction to ACLs

ACLs are lists of conditions that are applied to traffic that travels across a router interface. These lists tell the router what types of packets to accept or deny. ACLs can be created for all routed network protocols. ACLs filter network traffic and determine if routed packets are forwarded or blocked at the router interfaces. The ACL parameters that can be defined include source and destination addresses, protocols, and upper-layer port numbers. ACLs are created on a per-protocol, per-direction, and per-port basis. ACLs control traffic in one direction on an interface. Therefore, for every protocol, it is possible that two ACLs could be created, an inbound and an outbound. The following are some of the primary reasons to create ACLs:

- Limit network traffic and increase network performance
- Provide traffic flow control
- Provide a basic level of security for network access
- Decide which types of traffic are forwarded or blocked at the router interfaces
- Allow an administrator to control what areas a client can access on a network
- Screen certain hosts to either allow or deny access to part of a network
- Grant or deny user permission to access only certain types of files such as FTP or HTTP

The labs in CCNA 2 have allowed all traffic with no filtering. The students must understand the path, or know the source and destination address of the packets to apply the concept of an ACL. Review the OSI model and the protocols at each layer with the students. The reasons for ACLs and the methods that ACLs use to accomplish these functions may not be apparent to the students. ACLs may require some time to grasp. Do not rush through these sections. Give the students enough time to absorb this information. Encourage the students to use the labs to reinforce this knowledge. Encourage the students to experiment with various ACL scenarios.

## 11.1.2 How ACLs work

An ACL is a group of statements to permit or deny traffic on an inbound or outbound router interface. The order in which ACL statements are placed is important. The Cisco OS software tests the packet against each condition statement in order from the top of the list to the bottom. When a match is found in the list, an accept or reject action is performed and no other ACL statements are checked.

If additional condition statements are needed in an access list, the entire ACL must be deleted and recreated with the new condition statements. To simplify the process of revising an ACL it is a good idea to use a text editor such as Notepad and paste the ACL into the router configuration.

As a frame enters an interface, the router checks to see if the Layer 2 address matches or if it is a broadcast frame. If the frame address is accepted, the frame information is stripped off and the router checks for an ACL on the inbound interface.

As a review, ACL statements operate in sequential, logical order. If a condition match is true, the packet is permitted or denied and the rest of the ACL statements are not checked.

If all the ACL statements are unmatched, an implicit "deny any" statement is placed at the end of the list by default. Even though the "deny any" is not visible, it will deny any packets that are not matched in the ACL.

An exercise to use with the students is to look at each line of an ACL and ask the students what each line accomplishes. ACL statements are processed from the top down, one line at a time until a match is made. Remind students that at the end of each ACL is an implied deny all. Since the statements are processed sequentially, the order in which the commands are entered is extremely important. Changing the order of the statements can completely change what the ACL accomplishes.

### 11.1.3 Creating ACLs

ACLs are created in global configuration mode. When ACLs are configured on a router, each ACL must be uniquely identified. This is accomplished by assigning a number to it. After the access list is created, it must be assigned to the proper interface. ACLs are assigned to one or more interfaces and can filter inbound traffic or outbound traffic with the `ip access-group` command. The `ip access-group` command is issued in the interface configuration mode. To assign an access list to an interface, the direction of the traffic that the list will filter must also be defined. Traffic that enters an interface is filtered with an inbound access list. Traffic that leaves an interface is filtered with an outbound access list. To alter an ACL that contains numbered ACL statements, all the statements in the numbered ACL must be deleted with the `no access-list [list-number]` command.

The steps to configure an ACL are as follows:

```
rt1(config)#access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
<1000-1099> IPX SAP access list
<1100-1199> Extended 48-bit MAC address access list
<1200-1299> IPX summary address access list
<1300-1999> IP standard access list (expanded range)
<200-299>   Protocol type-code access list
<300-399>   DECnet access list
<600-699>   Appletalk access list
<700-799>   48-bit MAC address access list
<800-899>   IPX standard access list
<900-999>   IPX extended access list
<2000-2699> IP extended access list (expanded range)
rate-limit  Simple rate-limit specific access list
```

The students will need to memorize the ACL numbers.

```
rt1(config)#access-list 1 ?
deny  Specify packets to reject
permit Specify packets to forward
remark Access list entry comment

rt1(config)#access-list 1 permit ?
Hostname or A.B.C.D Address to match
any          Any source host
host         A single host address

rt1(config)#access-list 1 permit 192.168.0.1 ?
```

```
A.B.C.D Wildcard bits
log Log matches against this entry
<cr>
```

```
rtl(config)#access-list 1 permit 192.168.0.1 0.0.0.0 ?
log Log matches against this entry
<cr>
```

Give students a list of rules for access lists to help them understand this concept. Emphasize the following points:

- Use one access list for each protocol and for each direction.
- Place standard access lists closest to the destination.
- Place extended access lists closest to the source.
- Apply the "in" or "out" keyword as if from inside the router.
- Remember statements are processed sequentially from the top of the list until a match is found and if no match is found, the packet is denied.
- Remember there is an implicit "deny all" at the end of ACLs that will not appear in the configuration listing.
- Remember, the match condition is examined first and the permit or deny is examined ONLY if the match is true.
- List statements from specific references such as individual hosts to general references such as entire networks when access list logic overlaps.
- Do not work with an access list that is actively applied.
- Use Notepad or a similar text editor to create comments that outline the logic and then fill in the statements that perform the logic.
- Remember new lines are always added to the end of the access list.
- Use the **no access-list x** command to remove an entire list since it is not possible to selectively add and remove lines.
- Remember that an IP access list will send an ICMP host unreachable message to the sender of a rejected packet and will discard the packet.
- Use care when removing an access list. If the access list is applied to a production interface and it is removed, there may be a default "deny any" applied to the interface and all traffic will be halted. If the IOS defaults to "permit all", there will be no security or performance regulation.
- Remember outbound filters do not affect traffic that originates from the local router.

These rules will help students become successful with using ACLs. This is not an all-inclusive list and it can be presented in any order.

### 11.1.4 The function of a wildcard mask

A wildcard mask is paired with an IP address. The binary numbers one and zero in the mask are used to identify how the corresponding IP address bits should be handled. Wildcard masks are used for different purposes and follow different rules than subnet masks. Wildcard masks are designed to filter individual or multiple IP addresses to permit or deny access to resources based on the addresses. Another issue is that the ones and zeros mean something different in wildcard and subnet masks.

In the wildcard mask process, the IP address in the access-list statement has the wildcard mask applied to it. This creates the match value, which is used to determine if a packet should be processed by a specific ACL statement or sent to the next statement to be checked. There are two special keywords that are used in ACLs, the **any** and **host** options. The **any** option, substitutes for the IP address and 255.255.255.255 mask. This mask says to ignore the entire IP address, or to accept any addresses. The **host** option substitutes for the 0.0.0.0 mask. This mask states that all IP address bits must match or only one host is matched.

The wildcard mask of a complete subnet mask can be found by subtracting the subnet mask from 255.255.255.255.

For example, if the subnet mask is 255.255.240.0, the following equation would be used:

$$\begin{array}{r} 255.255.255.255 \\ - \underline{255.255.240.0} \\ 0. 0. 15.255 \end{array}$$

0.0.15.255 is the wildcard mask.

Emphasize the importance of assigning IP addresses within the subnetwork. If addresses are logically assigned based on system use or location, then an ACL can be created to permit or deny these hosts with a single statement. These logical host IP address assignments should be based on the binary bit patterns of each address. If these bit patterns have groupings of common bits in their addresses, then an address and wildcard mask can refer to this group of hosts. If addresses are made at random, then the creation of ACLs to refer to particular groups becomes difficult or impossible without a statement for each host. The IP address assignments should be consistent across the internetwork. For example, when a common group of bits is used to identify the network devices, these same bits should be used to identify all network devices in the internetwork.

### 11.1.5 Verifying ACLs

The **show ip interface** command displays IP interface information and indicates if any ACLs are set. The **show access-lists** command displays the contents of all ACLs on the router. To see a specific list, add the ACL name or number as an option for this command. The **show running-config** command will also reveal the access lists on a router and the interface assignment information. There are three common errors that students make when they create ACLs:

- Use incorrect wildcard masks
- Do not apply the ACL to an interface
- Filter in the wrong direction on an interface

To test an ACL, the students will need to know what traffic will be permitted, denied, and the path. Have students test for connectivity, apply the ACL, and then check the ACL to see if it works. The `show running-config` command should be used sparsely. Since lab configurations are relatively simple, the problems can usually be found rapidly with this command. However, students can become too dependent on it. When students troubleshoot the complex configurations of a production environment, this command will not be productive. The `show` and `debug` commands are the troubleshooting commands that should be used.

## 11.2 Access Control Lists (ACLs)

**Essential Labs:** 11.2.1a, 11.2.1b, 11.2.2a, 11.2.2b, and 11.2.3a

**Optional Labs:** 11.2.3b, 11.2.3c, and 11.2.6

**Core TIs:** 11.2.1, 11.2.2, 11.2.3, and 11.2.4

**Optional TIs:** 11.2.5 and 11.2.6

**Course-Level Claim:** Students can analyze, configure, implement, verify, and rectify access control lists within a router configuration.

**Certification-Level Claim:** Students can implement access lists, develop an access list to meet user specifications, troubleshoot an access list, and evaluate rules for packet control.

**Hands-on skills:** none

### 11.2.1 Standard ACLs

Standard ACLs check the source address of IP packets that are routed. The comparison will result in either permit or deny access for an entire protocol suite, based on the network, subnet, and host addresses. The standard version of the `access-list` global configuration command is used to define an IP standard ACL with a number in the range of 1 to 99. The full syntax of the standard ACL command is as follows:

```
Router(config)#access-list access-list-number {deny | permit}
source-address [source-wildcard] [log]
```

The `no` form of this command is used to remove a standard ACL:

```
Router(config)#no access-list access-list-number
```

A standard ACL only filters on the source address. The source can be a single host or an entire network. This is the major difference between a standard and extended ACL. Have the students discuss the ACL before they begin the labs. Draw a network, and tell the students to create a standard ACL to block a host or a network. Show students the path the packet will take from the source to the destination. At each router interface ask the students if the packet is going in or out of the interface. This information will be used when the `ip access-group` command is applied. Next, have the students decide on which router to configure an ACL. Remind them that a standard ACL is applied closest to the destination. When the students have the correct router, they must then decide which interface to apply the ACL to and if it should filter in or out. Ask the students which interface is closest to the destination and then ask if the packet is going in or out the interface.

## 11.2.2 Extended ACLs

Extended ACLs are used more often than standard ACLs because they provide a greater range of control. Extended ACLs check the source and destination packet addresses and also check for protocols and port numbers. This provides greater flexibility to define what the ACL will filter. Packets can be permitted or denied access based on where the packet originated and its destination or protocol types and port addresses. For a single ACL, multiple statements may be configured. The syntax for the extended ACL statement can get very long and will often wrap in the terminal window. The wildcards also have the option of using the **host** or **any** keywords in the command.

The extended ACL uses the source and destination address. Ask students what ports are used for FTP, Telnet, SMTP, HTTP, and DNS. The students need to have these ports memorized. The first part of the IP extended ACL is the same as the IP standard ACL. The number is within the range of 100 to 199.

```
rt1(config)#access-list 101 ?
deny    Specify packets to reject
dynamic Specify a DYNAMIC list of PERMITs or DENYs
permit  Specify packets to forward
remark  Access list entry comment
```

The permit or deny is the same as the standard.

```
rt1(config)#access-list 101 permit ?
<0-255> An IP protocol number
ahp     Authentication Header Protocol
eigrp   Cisco's EIGRP routing protocol
esp     Encapsulation Security Payload
gre     Cisco's GRE tunneling
icmp    Internet Control Message Protocol
igmp    Internet Gateway Message Protocol
igrp    Cisco's IGRP routing protocol
ip      Any Internet Protocol
ipinip  IP in IP tunneling
nos     KA9Q NOS compatible IP over IP tunneling
ospf    OSPF routing protocol
pcp     Payload Compression Protocol
pim     Protocol Independent Multicast
tcp     Transmission Control Protocol
udp     User Datagram Protocol
```

In an extended ACL, the protocol is listed after the permit or deny statement. Then enter the source address with the wildcard mask and destination address with the wildcard mask.

```
rt1(config)#access-list 101 permit tcp 172.16.0.1 0.0.0.0
192.168.0.0 0.0.255.255 ?
ack     Match on the ACK bit
eq      Match only packets on a given port number
established Match established connections
fin     Match on the FIN bit
gt      Match only packets with a greater port number
log     Log matches against this entry
log-input Log matches against this entry, including input
interface
lt      Match only packets with a lower port number
neq     Match only packets not on a given port number
```

```

precedence  Match packets with given precedence value
psh        Match on the PSH bit
range      Match only packets in the range of port numbers
rst        Match on the RST bit
syn        Match on the SYN bit
time-range Specify a time-range
tos        Match packets with given TOS value
urg        Match on the URG bit
<cr>

```

Next enter **eq**, **gt** or any of the above. The **eq**, **gt** and **lt** define ranges of port numbers. The students need to know the standard port numbers and if they use TCP or UDP. At the end of every ACL is the implied deny all statement. A common error is failure to enter a permit statement. If the ACL does not contain a permit statement, nothing will be permitted.

There are two ways to design security with ACLs. The first is to create an ACL that specifically denies potentially harmful traffic and permits all other traffic. Most of the ACL statements will consist of deny statements with a **permit any** command as the last entry in the list. This generally has the advantage of being easier to create and has fewer lines. It is also less secure than the other method.

The second method is to only permit traffic that is specified as appropriate. With this type of list, every type of traffic that is permissible requires a line in the list to permit it. All other traffic will be denied by the implicit deny at the bottom of the list. These lists consist of primarily permit statements and do not have a permit any at the end of the list. While these lists require more planning and lines of code, they are typically more secure. The maintenance for this type of list is usually triggered by the implementation of a new application or service that requires access by hosts on the internetwork.

### 11.2.3 Named ACLs

IP named ACLs were introduced in Cisco IOS Software Release 11.2 to allow standard and extended ACLs to be given names instead of numbers.

The advantages of a named access list are as follows:

- Intuitively identify an ACL with an alphanumeric name
- Eliminates the limit of 99 simple and 100 extended ACLs
- Ability to modify ACLs without deleting and then reconfiguring them

It is important to note that a named access list will allow the deletion of statements but will only allow for statements to be inserted at the end of a list.

The configuration of a named ACL is very similar to the configuration of a standard or extended ACL. The first difference is that instead of starting the command with **access-list** the named ACL uses **ip access-list**:

```

rt1(config)#ip access-list ?
  extended  Extended Access List
  log-update Control access list log updates
  logging   Control access list logging
  standard  Standard Access List

```

Then enter **extended** or **standard**:

```
rt1(config)#ip access-list extended ?
<100-199> Extended IP access-list number
WORD      Access-list name
```

The name used is **named\_ACL**:

```
rt1(config)#ip access-list extended named_ACL
rt1(config-ext-nacl)#

rt1(config-ext-nacl)#?
Ext Access List configuration commands:
default Set a command to its defaults
deny Specify packets to reject
dynamic Specify a DYNAMIC list of PERMITS or DENYS
evaluate Evaluate an access list
exit Exit from access-list configuration mode
no Negate a command or set its defaults
permit Specify packets to forward
remark Access list entry comment
```

From this point the ACL will work like any other extended ACL.

## 11.2.4 Placing ACLs

ACLs are used to control traffic by filtering packets and eliminating unwanted traffic on a network. Another important consideration of when ACLs are implemented is the placement of the access list. The ACL should be placed where it has the greatest impact on increased efficiency. The general rule is to put the extended ACLs as close as possible to the source of the traffic that is denied. Standard ACLs do not specify destination addresses, so they should be placed as close to the destination as possible. For example, a standard ACL should be placed on Fa0/0 of Router D to prevent traffic from Router A.

Administrators can only place access lists on devices that they control.

A standard ACL should be placed close to the destination. First, have the students decide which router is closest to the destination and then pick which interface is the closest to the destination. An ACL can be applied to any of the interfaces, but if an ACL is applied to the wrong interface a negative result is possible. The extended ACL should be placed closest to the source. Have the students decide which router is closest and then choose the correct interface. The **in** or **out** commands also need to be correct or the ACL will not work. Students commonly forget to apply the ACL or filter in the wrong direction.

## 11.2.5 Firewalls

A firewall is an architectural structure that exists between the user and the outside world to protect the internal network from intruders. A network firewall usually consists of several different machines that work together to prevent unwanted and illegal access. ACLs should be used in firewall routers, which are often positioned between the internal network and an external network, such as the Internet.

ACLs must be configured on border routers, which are routers situated on the boundaries of the network, to provide security benefits. CCNA 2 will cover standard, extended, and named ACLs. Other types will be covered in the CCNP classes.



## 11.2.6 Restricting virtual terminal access

Standard and extended access lists apply to packets that travel through a router. They are not designed to block packets that originate within the router. By default, an outbound Telnet extended access list does not prevent router initiated Telnet sessions. This type of ACL controls which users can telnet into a remote router. To test this in the labs, have students configure routers and telnet into a remote router to test connectivity. Configure and apply the ACL to the vty lines to deny access. Then test the Telnet again. Here are the commands to configure virtual terminal access:

```
Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255  
Rt1(config)#access-list 2 permit 172.16.2.0 0.0.0.255  
Rt1(config)#access-list 2 deny any
```

Here are the commands to apply the access list:

```
Rt1(config)#line vty 0 4  
Rt1(config-line)#login  
Rt1(config-line)#password secret  
Rt1(config-line)#access-class 2 in
```

## Module 11 Summary

Before students take the final exam, they should have mastered the configuration and placement of standard and extended IP access-lists.

Online assessment options include the end-of-module online quiz in the curriculum and the online Module 11 exam. Formative assessments such as short paper quizzes that instruct students to write out an access list in response to a scenario may help students achieve mastery.

Students should understand the following main points:

- ACLs perform several functions within a router, which includes the implementation of security access procedures.
- ACLs are used to control and manage traffic.
- For some protocols, two ACLs can be applied to an interface, an inbound ACL and an outbound ACL.
- After a packet is matched to an ACL statement, it can be denied or permitted access to the router.
- Wildcard mask bits use the number one (1) and the number zero (0) to identify how to treat the corresponding IP address bits.
- Access list creation and application is verified through the use of various IOS **show** commands.
- The two main types of ACLs are standard and extended.
- Named ACLs allow access lists to be identified by names instead of numbers.
- ACLs can be configured for all routed network protocols.
- ACLs are placed where they allow the most efficient control.
- ACLs are typically used in firewall routers.
- Access lists can also restrict virtual terminal access to the router.

# IV. Case Study

## Overview and Objectives

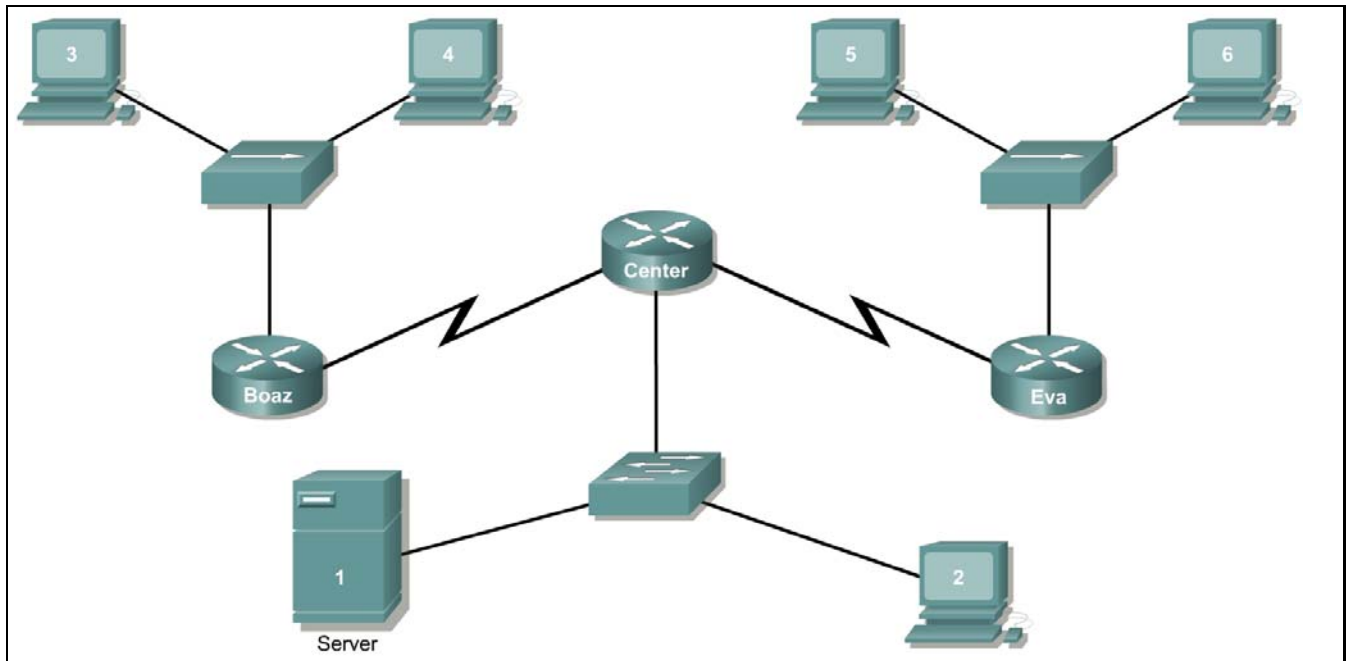
This case study allows students to complete a network design, implementation, and troubleshooting project using the skills gained in CCNA 2. Students will use the skills that have already been developed to use, make, and connect the proper cabling to the appropriate devices.

It is crucial to read and understand the scenarios to make sure that all requirements are fulfilled. Each scenario guides the student through the proper steps to ensure that the project is completed properly.

This case study requires the student to accomplish the following tasks:

- Set up the physical layout of the network using the diagram and accompanying narrative
- Correctly configure the routers with a basic router configuration
- Set up a TFTP server on one of the workstations
- Create and apply access control lists on the appropriate router(s) and interface(s)
- Troubleshoot and test all connectivity and access control lists
- Provide detailed documentation in a prescribed form, as listed in the deliverables section

## Scenario and Phase 1: Project Description



A company has several people responsible for maintaining various sections of the internetwork infrastructure. Many technicians have done an excellent job with the small portion for which they are responsible.

One of the other network associates who was responsible for a larger portion of the infrastructure suddenly left the company. This left redesign and implementation on this portion of the internetwork unfinished. A technician is given the task to complete the design and implementation of the unfinished network.

After taking home the documentation to study over the weekend, it is apparent to the technician why the network associate left suddenly. The few documents that existed were poorly written. So during the weekend the technician reconstructs the diagram above from an existing diagram that was found. It represents the new internetwork design. It shows the planned routers, hubs/switches, circuits, and the servers/workstations at each site. The server at the Center site is a file server accessed only by workstations on this internetwork. The workstation at the Center site is used to manage all routers on the internetwork.

After returning to work Monday morning, the technician presents the new diagram to the Network Infrastructure Team Leader that assigned the project. After discussion, it is determined that new documentation must be developed for the project. The Team Leader, the instructor, must approve the documentation at each phase of the process. Use the following information to implement the network.

Network address \_\_\_\_\_

Required number of subnets \_\_\_\_\_

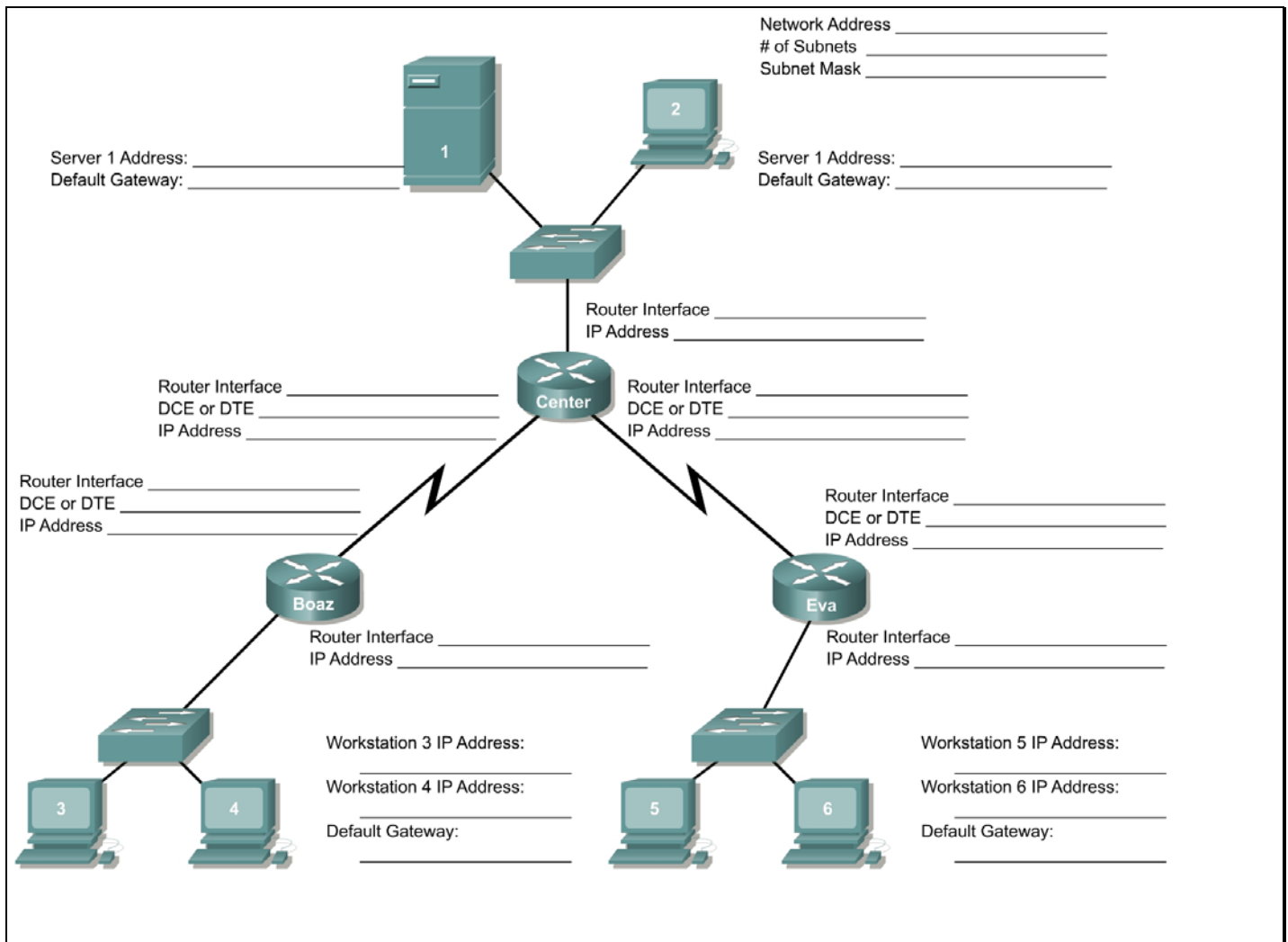
Routing protocol \_\_\_\_\_

## Phase 2: IP Addressing

Now that the basic plan is in place, the team leader assigns the technician to develop a prototype for the new internetwork. Use the network address assigned along with the subnetting requirements, to subnet the network. From the IP addressing scheme, assign IP addresses to the appropriate interfaces on all routers and computers in the internetwork. Use the diagram below as a guide. Obtain approval of this phase of development from the team leader before proceeding to Phase 3.

Instructor approval \_\_\_\_\_ Date \_\_\_\_\_

### Network Diagram - IP Addressing



### Phase 3: Basic Router and Workstation Configuration

After the team leader inspects the prototype cabling, the technician is assigned to create a basic configuration on the router and workstations.

Use the diagram and planning sheets to create a basic configuration for the router. The checklist below will help keep track of the configuration process.

	<b>Boaz</b>	<b>Center</b>	<b>Eva</b>
<b>Hostname</b>			
<b>Console Password</b>			
<b>Secret Password</b>			
<b>VTY Password</b>			
<b>Serial 0/0 IP address</b>			
<b>Serial 0/1 IP address</b>			
<b>*Serial 0/0 Clock Rate</b>			
<b>*Serial 0/1 Clock Rate</b>			
<b>Fa 0/0 IP address</b>			
<b>Fa 0/1 IP address</b>			
<b>Enable the interfaces</b>			
<b>Add Routing Protocol</b>			
<b>Add Network Statements</b>			

**Note** \*: As needed

Table continued on next page

	<b>Boaz</b>	<b>Center</b>	<b>Eva</b>
<b>* Host Table - contains all routers and servers</b>			
<b>Message of the Day</b>			
<b>Serial 0/0 description</b>			
<b>Serial 0/1 description</b>			
<b>Fa 0/0 description</b>			
<b>Fa 0/1 description</b>			

Instructor approval \_\_\_\_\_ Date \_\_\_\_\_

## Phase 4: Access Control Lists

While testing the network, the team leader discovers that security has not been planned for the network. If the network configuration were installed as designed, any network user would be able to access all network devices and workstations.

The team leader asks the technician to add access control lists (ACLs) to the routers. The team leader has some suggestions for developing the security. Before the ACLs are added, backup the current router configuration. Also, make sure there is complete connectivity throughout the network before any of the ACLs are applied.

The following conditions must be taken into consideration when creating the ACLs:

- Workstation 2 and File Server 1 are on the management network. Any device on the management network can access any other device on the entire network.
- Workstations on Eva and Boaz LANs are not permitted outside of their subnet except to access File Server 1.
- Each router can telnet to the other routers and access any device on the network.

The team lead asks the technician to write down a short summary of the purpose of each ACL, the interfaces upon which they will be applied, and the direction of the traffic. Then list the exact commands that will be used to create and apply the ACLs to the router interfaces.

Before the ACLs are configured on the routers, review each of the following test conditions and make sure that the ACLs will perform as expected:

Telnet from Boaz to Eva	SUCCESSFUL
Telnet from Workstation 4 to Eva	BLOCKED
TELNET from Workstation 5 to Boaz	BLOCKED
TELNET from Workstation 2 to Boaz	SUCCESSFUL
TELNET from Workstation 2 to Eva	SUCCESSFUL
Ping from Workstation 5 to File Server 1	SUCCESSFUL
Ping from Workstation 3 to File Server 1	SUCCESSFUL
Ping from Workstation 3 to Workstation 4	SUCCESSFUL
Ping from Workstation 5 to Workstation 6	SUCCESSFUL
Ping from Workstation 3 to Workstation 5	BLOCKED
Ping from Workstation 2 to Workstation 5	SUCCESSFUL
Ping from Workstation 2 to Workstation 3	SUCCESSFUL
Ping from Router Eva to Workstation 3	SUCCESSFUL
Ping from Router Boaz to Workstation 5	SUCCESSFUL



## Phase 5: Documenting the Network

In order to support the network properly, documentation is required. Create documentation that is logically organized to make troubleshooting simpler.

### Configuration management documentation

	<b>Boaz</b>	<b>Center</b>	<b>Eva</b>
<code>show cdp neighbors</code>			
<code>show ip route</code>			
<code>show ip protocol</code>			
<code>show ip interface brief</code>			
<code>show version</code>			
<code>show hosts</code>			
<code>show startup config</code>			

### Security management documentation

	<b>Boaz</b>	<b>Center</b>	<b>Eva</b>
<code>show ip interface</code>			
<code>show ip access lists</code>			

Instructor approval \_\_\_\_\_ Date \_\_\_\_\_

## Case Study Deliverables

The key lesson of this case study is the importance of thorough and clear documentation. There should be two types of documentation completed.

### General Documentation:

- A complete narrative of the project should be typed using word processing software. Since the scenarios break up the entire task into pieces, take care to address each scenario task so that any layperson could understand that particular task.
- Microsoft Excel or another spreadsheet program could be used to simply list the equipment and serial numbers.
- Cisco Network Designer (CND), Microsoft Visio, or any paint program could be used to draw the network.
- Provide documentation that specifies how the security was tested. A plan for monitoring the network should also be included.

### Technical Documentation:

The technical documentation should include details of the network topology. Use CND, Visio, or any paint program to draw the network.

Use the tables in the working copy of the case study as a reference, and enter all table information into a spreadsheet program such as Microsoft Excel. The spreadsheet should include the following details:

- IP addressing of all interfaces
- DCE/DTE information
- Router passwords
- Interface descriptions
- IP addressing and gateway assignments for all PCs

The actual access control lists, or router commands sequence, should be included in this documentation using a word processing program. Be sure to include the router interface the list is applied to and the direction.

Document the use of a routing protocol.

Router output from the following commands should be captured and placed into this documentation:

- show cdp neighbors
- show ip route
- show ip protocol

- show ip interface
- show version
- show hosts
- show startup-config
- show ip access-list

## Case Study – Instructor Notes

### Phase 1: Project Description

This phase of the case study can begin early in the semester, as students should be familiar with subnetting.

The entire case study should be discussed in class so that all students understand that the purpose of this study is not only to practice configuration and troubleshooting, but also to learn how to document their work. The following are some good web sites that will help the students' understanding of documentation:

<http://www.ittoolkit.com/articles/tech/importofdocs.htm>

<http://www.serverwatch.com/tutorials/article.php/1475021>

[http://www.ethermanage.com/ethernet/100quickref/ch14qr\\_16.html](http://www.ethermanage.com/ethernet/100quickref/ch14qr_16.html)

<http://tampabay.bizjournals.com/tampabay/stories/1997/11/24/smallb2.html>

The network address assigned should be one of the private IP address ranges or a subnet of one:

Class	Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

The routing protocol should be IGRP. The first part of Phase 1 should probably be completed as a class so that students understand the purpose of the case study. Along with a discussion of Phase 1, the deliverable piece should also be covered. The instructor should decide whether or not this is a group project. Certainly each student should be capable of deciding on IP addresses of interfaces after the IP scheme has been chosen.

The Network Diagram - IP Addressing on page 4 is the first document that should be approved by the instructor.

### Phase 2: IP Addressing

This Phase of the case study should be due after module 4 or 5 is completed.

Students should recreate the drawing during this Phase using CDN, Visio, or a paint program. In the drawing the students should be advised to insert the appropriate interface connections on the routers. The drawing should be approved by the instructor.

The following topics can be used for class discussion:

- The reasons for using private IP addressing

- The concept of reserved address space for routers, servers, and hosts
- The reasons for developing an IP address scheme to allow for future growth

### Phase 3: Basic Router and Workstation Configuration

This Phase should be completed after students feel comfortable with basic router configuration, sometime after Module 7.

Students should be somewhat familiar with router configuration, and understand the basic requirements. The checklist included in Phase 3 will help them to include the essential items for router configuration. The student should select which workstation is to be the TFTP server. They must understand which devices need access to the TFTP server. Students should be guided to complete the chart in Phase 3, and then have the instructor approve the configuration.

After instructor approval, students should enter their configurations and test them on the routers.

### Phase 4: Access Control Lists

This Phase should be completed after Module 11.

This is a most critical portion of the case study. Students must develop an access control list on paper first, then type the ACL into a word processing application. The instructor should guide the students through the process of copying and pasting ACLs into the router configuration.

### Phase 5: Documenting the Network

If the documentation requirements are clear to the students at the beginning of the case study, the final Phase will have been completed throughout the life of the case study. The Phase will help to reiterate the purpose of documentation, that it should be done continually and revisited, not only once.

During the last phase the deliverables list should be discussed again to make sure the student understands the requirements.

### Optional

An additional Phase could be a reflection phase so that the student can look objectively at this case study. Questions might include: “Why have two types of documentation?”, “What happens when a piece of equipment fails?”, and so forth.

## Case Study – Instructor Sample Outputs

### Phase 5: Documenting the Network – Sample outputs Boaz (2500)

#### Configuration Management documentation – Boaz (2500)

```
Boaz#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route  
Bridge
```

```
          S - Switch, H - Host, I - IGMP
```

```
Device ID      Local Intrfce  Holdtme  Capability  Platform  Port  ID  
Centre          Ser 0      120      R          2500      Ser 0
```

```
Boaz#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -  
BGP
```

```
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
```

```
default
```

```
      U - per-user static route
```

```
Gateway of last resort is not set
```

```
      172.16.0.0/16 is subnetted, 4 subnets
```

```
I      172.16.128.0 [100/10476] via 172.16.64.1, 00:00:20, Serial0
```

```
I      172.16.32.0 [100/8576] via 172.16.64.1, 00:00:20, Serial0
```

```
C      172.16.96.0 is directly connected, Ethernet0
```

```
C      172.16.64.0 is directly connected, Serial0
```

```
Boaz#show ip protocols
```

```
Routing Protocol is "igrp 11"
```

```
  Sending updates every 90 seconds, next due in 34 seconds
```

```
  Invalid after 270 seconds, hold down 280, flushed after 630
```

```
  Outgoing update filter list for all interfaces is not set
```

```
  Incoming update filter list for all interfaces is not set
```

```
  Default networks flagged in outgoing updates
```

```
  Default networks accepted from incoming updates
```

```
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```
  IGRP maximum hopcount 100
```

```
  IGRP maximum metric variance 1
```

```
  Redistributing: igrp 11
```

```
  Routing for Networks:
```

```
    172.16.0.0
```

```
  Routing Information Sources:
```

```
    Gateway      Distance  Last Update
```

```
    172.16.64.1      100    00:00:37
```

```
  Distance: (default is 100)
```

Boaz#**show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	172.16.96.1	YES	manual	up	up
Serial0	172.16.64.2	YES	manual	up	up
Serial1	unassigned	YES	unset	administratively down	down

Boaz#**show version**

Cisco Internetwork Operating System Software  
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE SOFTWARE (fcl)

Copyright (c) 1986-1996 by Cisco Systems, Inc.  
Compiled Mon 05-Aug-96 11:48 by mkamson  
Image text-base: 0x0303794C, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE  
ROM: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE (fcl)

Boaz uptime is 5 hours, 6 minutes  
System restarted by power-on  
System image file is "flash:igs-j-l.111-5", booted via flash

Cisco 2500 (68030) processor (revision N) with 6144K/2048K bytes of memory.

Processor board ID 22650091, with hardware revision 00000000  
Bridging software.

SuperLAT software copyright 1990 by Meridian Technology Corp).

X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.

TN3270 Emulation software (copyright 1994 by TGV Inc).

1 Ethernet/IEEE 802.3 interface.

2 Serial network interfaces.

32K bytes of non-volatile configuration memory.

8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

Boaz#**show hosts**

Default domain is not set

Name/address lookup uses domain service

Name servers are 255.255.255.255

Host	Flags	Age	Type	Address(es)
Centre	(perm, OK)	4	IP	172.16.64.1 172.16.128.1 172.16.32.1
Boaz	(perm, OK)	4	IP	172.16.64.2 172.16.96.1
Eva	(perm, OK)	4	IP	172.16.128.2 172.16.160.1

```

Boaz#show startup-config
Using 1090 out of 32762 bytes
!
version 11.1
service slave-log
service udp-small-servers
service tcp-small-servers
!
hostname Boaz
!
enable secret 5 $1$5EE4$v86z7o8zMLehnIWA0T7LB/
!
!
interface Ethernet0
  description Boaz LAN workgroup interface
  ip address 172.16.96.1 255.255.224.0
  ip access-group 101 in
  no keepalive
!
interface Serial0
  description Boaz WAN interface to Centre
  ip address 172.16.64.2 255.255.224.0
  no fair-queue
!
interface Serial1
  no ip address
  shutdown
!
router igrp 11
  network 172.16.0.0
!
ip host Centre 172.16.64.1 172.16.128.1 172.16.32.1
ip host Boaz 172.16.64.2 172.16.96.1
ip host Eva 172.16.128.2 172.16.160.1
no ip classless
access-list 101 permit ip 172.16.96.0 0.0.31.255 host 172.16.32.5
access-list 101 permit ip 172.16.96.0 0.0.31.255 172.16.96.0
0.0.31.255
access-list 101 deny tcp 172.16.96.0 0.0.31.255 any eq telnet
access-list 101 deny icmp 172.16.96.0 0.0.31.255 any
!
banner motd ^CWarning: This is a SECURE SYSTEM: UNAUTHORIZED USERS
will be prosecuted.^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
line aux 0
line vty 0 4
  password cisco
  login
!
end

Boaz#

```



## Security Management documentation – Boaz (2500)

```
Boaz#show ip interface
Ethernet0 is up, line protocol is up
  Internet address is 172.16.96.1/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is 101
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled
Serial0 is up, line protocol is up
  Internet address is 172.16.64.2/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled
Serial1 is administratively down, line protocol is down
  Internet protocol processing disabled
```

### Boaz#show ip access-lists

```
Extended IP access list 101
  permit ip 172.16.96.0 0.0.31.255 host 172.16.32.5 (7 matches)
  permit ip 172.16.96.0 0.0.31.255 172.16.96.0 0.0.31.255 (72 matches)
```

```
deny tcp 172.16.96.0 0.0.31.255 any eq telnet
deny icmp 172.16.96.0 0.0.31.255 any (8 matches)
Boaz#
```

## Phase 5: Documenting the Network – Sample outputs Centre (2500)

### Configuration Management documentation

```
Centre#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route  
Bridge
```

```
S - Switch, H - Host, I - IGMP
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Boaz	Ser 0	153	R 2500	Ser 0	
Eva	Ser 1	140	R 2500	Ser 1	

```
Centre#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -  
BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
```

```
default
```

```
U - per-user static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/16 is subnetted, 4 subnets
```

```
C 172.16.128.0 is directly connected, Serial1
```

```
C 172.16.32.0 is directly connected, Ethernet0
```

```
I 172.16.96.0 [100/8576] via 172.16.64.2, 00:00:57, Serial0
```

```
C 172.16.64.0 is directly connected, Serial0
```

```
Centre#show ip protocol
```

```
Routing Protocol is "igrp 11"
```

```
Sending updates every 90 seconds, next due in 50 seconds
```

```
Invalid after 270 seconds, hold down 280, flushed after 630
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Default networks flagged in outgoing updates
```

```
Default networks accepted from incoming updates
```

```
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```
IGRP maximum hopcount 100
```

```
IGRP maximum metric variance 1
```

```
Redistributing: igrp 11
```

```
Routing for Networks:
```

```
172.16.0.0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update
172.16.128.2	100	00:40:35
172.16.64.2	100	00:01:07

```
Distance: (default is 100)
```

```
Centre#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	172.16.32.1	YES	manual	up	up
Ethernet1	unassigned	YES	unset	administratively down	down
Serial0	172.16.64.1	YES	manual	up	up
Serial1	172.16.128.1	YES	manual	up	up

Centre#**show version**

Cisco Internetwork Operating System Software  
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE SOFTWARE  
(fcl)  
Copyright (c) 1986-1996 by Cisco Systems, Inc.  
Compiled Mon 05-Aug-96 11:48 by mkamson  
Image text-base: 0x0303794C, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c)XB2, PLATFORM SPECIFIC RELEASE  
SOFTWARE (fcl)  
ROM: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB2,  
PLATFORM SPECIFIC RELEASE SOFTWARE (fcl)

Centre uptime is 5 hours, 18 minutes  
System restarted by power-on  
System image file is "flash:igs-j-l.111-5", booted via flash

Cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of  
memory.  
Processor board ID 02782545, with hardware revision 00000000  
Bridging software.  
SuperLAT software copyright 1990 by Meridian Technology Corp).  
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.  
TN3270 Emulation software (copyright 1994 by TGV Inc).  
2 Ethernet/IEEE 802.3 interfaces.  
2 Serial network interfaces.  
32K bytes of non-volatile configuration memory.  
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

Centre#**show host**

Default domain is not set  
Name/address lookup uses domain service  
Name servers are 255.255.255.255

Host	Flags	Age	Type	Address(es)
Centre	(perm, OK)	4	IP	172.16.64.1 172.16.128.1 172.16.32.1
Boaz	(perm, OK)	4	IP	172.16.64.2 172.16.96.1
Eva	(perm, OK)	4	IP	172.16.128.2 172.16.160.1

Centre#**show startup-config**

Using 907 out of 32762 bytes  
!  
version 11.1  
service slave-log  
service udp-small-servers  
service tcp-small-servers  
!  
hostname Centre  
!  
enable secret 5 \$l\$MlW5\$wj.I9efI57i0AxLPf4qOj/  
!  
!  
interface Ethernet0  
  description Centre LAN workgroup interface  
  ip address 172.16.32.1 255.255.224.0  
!  
interface Ethernet1

```
no ip address
shutdown
!
interface Serial0
description Centre WAN interface to Boaz
ip address 172.16.64.1 255.255.224.0
no fair-queue
clockrate 56000
!
interface Serial1
description Centre WAN interface to Eva
ip address 172.16.128.1 255.255.224.0
clockrate 56000
!
router igrp 11
network 172.16.0.0
!
ip host Centre 172.16.64.1 172.16.128.1 172.16.32.1
ip host Boaz 172.16.64.2 172.16.96.1
ip host Eva 172.16.128.2 172.16.160.1
no ip classless
!
banner motd ^CThis is a SECURE SYSTEM. UNAUTHORIZED USERS will be
prosecuted.^C
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
end

Centre#
```

## Security Management documentation – Centre (2500)

```
Centre#show ip interface
Ethernet0 is up, line protocol is up
  Internet address is 172.16.32.1/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled
Ethernet1 is administratively down, line protocol is down
  Internet protocol processing disabled
Serial0 is up, line protocol is up
  Internet address is 172.16.64.1/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled
Serial1 is up, line protocol is up
  Internet address is 172.16.128.1/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
```

```
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP multicast fast switching is enabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
```

```
Centre#show ip access-lists
      <none applied>
```

```
Centre#
```

## Phase 5: Documenting the Network – Sample outputs Eva (2500)

### Configuration Management documentation – Eva (2500)

Eva#**show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Centre	Ser 1	147	R	2500	Ser 1

Eva#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate  
default  
U - per-user static route

Gateway of last resort is not set

172.16.0.0/16 is subnetted, 4 subnets  
C 172.16.128.0 is directly connected, Serial1  
I 172.16.32.0 [100/8576] via 172.16.128.1, 00:01:17, Serial1  
I 172.16.96.0 [100/10576] via 172.16.128.1, 00:01:18, Serial1  
I 172.16.64.0 [100/10476] via 172.16.128.1, 00:01:18, Serial1

Eva#**show ip protocol**

Routing Protocol is "igrp 11"  
Sending updates every 90 seconds, next due in 24 seconds  
Invalid after 270 seconds, hold down 280, flushed after 630  
Outgoing update filter list for all interfaces is not set  
Incoming update filter list for all interfaces is not set  
Default networks flagged in outgoing updates  
Default networks accepted from incoming updates  
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0  
IGRP maximum hopcount 100  
IGRP maximum metric variance 1  
Redistributing: igrp 11  
Routing for Networks:  
172.16.0.0  
Routing Information Sources:  
Gateway Distance Last Update  
172.16.128.1 100 00:00:07  
Distance: (default is 100)

Eva#**show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	172.16.160.1	YES	manual	up	down
Serial0	unassigned	YES	unset	administratively down	down
Serial1	172.16.128.2	YES	manual	up	up

Eva#**show version**

Cisco Internetwork Operating System Software  
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE SOFTWARE  
(fcl)  
Copyright (c) 1986-1996 by cisco Systems, Inc.  
Compiled Mon 05-Aug-96 11:48 by mkamson



Image text-base: 0x0303794C, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE  
ROM: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE  
SOFTWARE (fcl)

Eva uptime is 5 hours, 4 minutes  
System restarted by reload  
System image file is "flash:igs-j-1.111-5", booted via flash

Cisco 2500 (68030) processor (revision N) with 6144K/2048K bytes of  
memory.

Processor board ID 06147980, with hardware revision 00000000  
Bridging software.

SuperLAT software copyright 1990 by Meridian Technology Corp).

X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.

TN3270 Emulation software (copyright 1994 by TGV Inc).

1 Ethernet/IEEE 802.3 interface.

2 Serial network interfaces.

32K bytes of non-volatile configuration memory.

8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

Eva#**show hosts**

Default domain is not set

Name/address lookup uses static mappings

Host	Flags	Age	Type	Address(es)
Boaz	(perm, OK)	4	IP	172.16.64.2 172.16.96.1
Centre	(perm, OK)	4	IP	172.16.64.1 172.16.128.1 172.16.32.1

```

Eva#show startup-config
Using 1156 out of 32762 bytes
!
version 11.1
service slave-log
service udp-small-servers
service tcp-small-servers
!
hostname Eva
!
enable secret 5 $1$ejwr$qcHMWf3GAiWytPceeWKly0
!
ip subnet-zero
!
interface Ethernet0
  description Eva LAN workgroup interface
  ip address 172.16.160.1 255.255.224.0
  ip access-group 103 in
!
interface Serial0
  no ip address
  shutdown
  no fair-queue
!
interface Serial1
  description Eva WAN interface to Centre
  ip address 172.16.128.2 255.255.224.0
!
router igrp 11
  network 172.16.0.0
!
ip host Boaz 172.16.64.2 172.16.96.1
ip host Centre 172.16.64.1 172.16.128.1 172.16.32.1
no ip classless
ip http server
access-list 103 permit ip 172.16.160.0 0.0.31.255 host 172.16.32.5
access-list 103 permit ip 172.16.160.0 0.0.31.255 172.16.160.0
0.0.31.255
access-list 103 deny tcp 172.16.160.0 0.0.31.255 any eq telnet
access-list 103 deny icmp 172.16.160.0 0.0.31.255 any
!
banner motd ^CWarning: This is a SECURE SYSTEM. UNAUTHORIZED USER will
be prosecuted.^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
  password cisco
  login
line vty 0 4
  password cisco
  login
!
end

Eva#

```

## Security Management documentation – Eva (2500)

```
Eva#show ip interface
Ethernet0 is up, line protocol is down
  Internet address is 172.16.160.1/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is 103
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled
Serial0 is administratively down, line protocol is down
  Internet protocol processing disabled
Serial1 is up, line protocol is up
  Internet address is 172.16.128.2/19
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP multicast fast switching is enabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  Gateway Discovery is disabled
  Policy routing is disabled

Eva#show ip access-lists
Extended IP access list 103
  permit ip 172.16.160.0 0.0.31.255 host 172.16.32.5 (15 matches)
```

```
    permit ip 172.16.160.0 0.0.31.255 172.16.160.0 0.0.31.255 (225
matches)
    deny tcp 172.16.160.0 0.0.31.255 any eq telnet
    deny icmp 172.16.160.0 0.0.31.255 any (20 matches)
Eva#
```

## V. Appendices:

A) Cisco Online Tools and Utilities

B) Instructional Best Practices

## Appendix A: Cisco Online Tools and Utilities

Cisco Systems offer a wide range of online documents and tools to assist in the configuration, troubleshooting, and optimization of routers and switches. These resources can be found on the Cisco Technical Assistance Center (TAC) website at <http://www.cisco.com/tac>. To learn more about the Cisco TAC website visit [http://www.cisco.com/public/news\\_training/tac\\_overview.html](http://www.cisco.com/public/news_training/tac_overview.html). This document introduces ten valuable resources that are available to users at cisco.com.

A cisco.com user ID and password is required to access all of the tools on the Cisco TAC website. A user ID and password can be obtained with a valid Cisco service contract at <http://tools.cisco.com/RPF/register/register.do>.

# 1 Output Interpreter

The screenshot shows the Cisco Systems website's 'Output Interpreter' page. At the top, there is a navigation bar with the Cisco logo, a search bar, and links for Home, Logged In, Profile, Contacts & Feedback, Help, and Site Map. Below this is a 'Technical Support' dropdown menu with a 'GO' button. The main content area is titled 'Output Interpreter' and features a yellow callout box with the text: 'Check out this new functionality! Now you can paste your PIX show tech-support or running configuration into Output Interpreter to automatically convert 'conduct', 'outbound' or 'apply' statements to 'access-list' statements.' Below the callout, there is a paragraph explaining the tool's purpose: 'The Output Interpreter is a troubleshooting tool that will report potential problems by analyzing supported show command output. View an [example of results generated](#) by this tool.' This is followed by a note: 'Not all commands are supported by Output Interpreter. Look up supported commands relevant to your issue in the following lists:' and two bullet points: 'List of Supported "Show" Commands' and 'Problem to Command Mappings'. At the bottom of the main content area, there is a form titled 'Enter "show" command(s) output from your device for analysis.' with instructions to 'Paste the output of your command(s) in the field below:' and a large text area for input. Below the text area, there is a 'Browse...' button for uploading files.

Output Interpreter is a Web-based application that provides a troubleshooting analysis and a course of action for a router, switch, or PIX device. Output Interpreter uses a collection of **show** command output to perform the analysis. Users paste the output of one or more supported commands into Output Interpreter to receive a report that includes errors, warnings, and relevant troubleshooting information. The report also includes crash analysis and error message decodes, which were previously supported by the Stack Decoder and the Error Message Decoder tools.

<http://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

## 2 Error Message Decoder

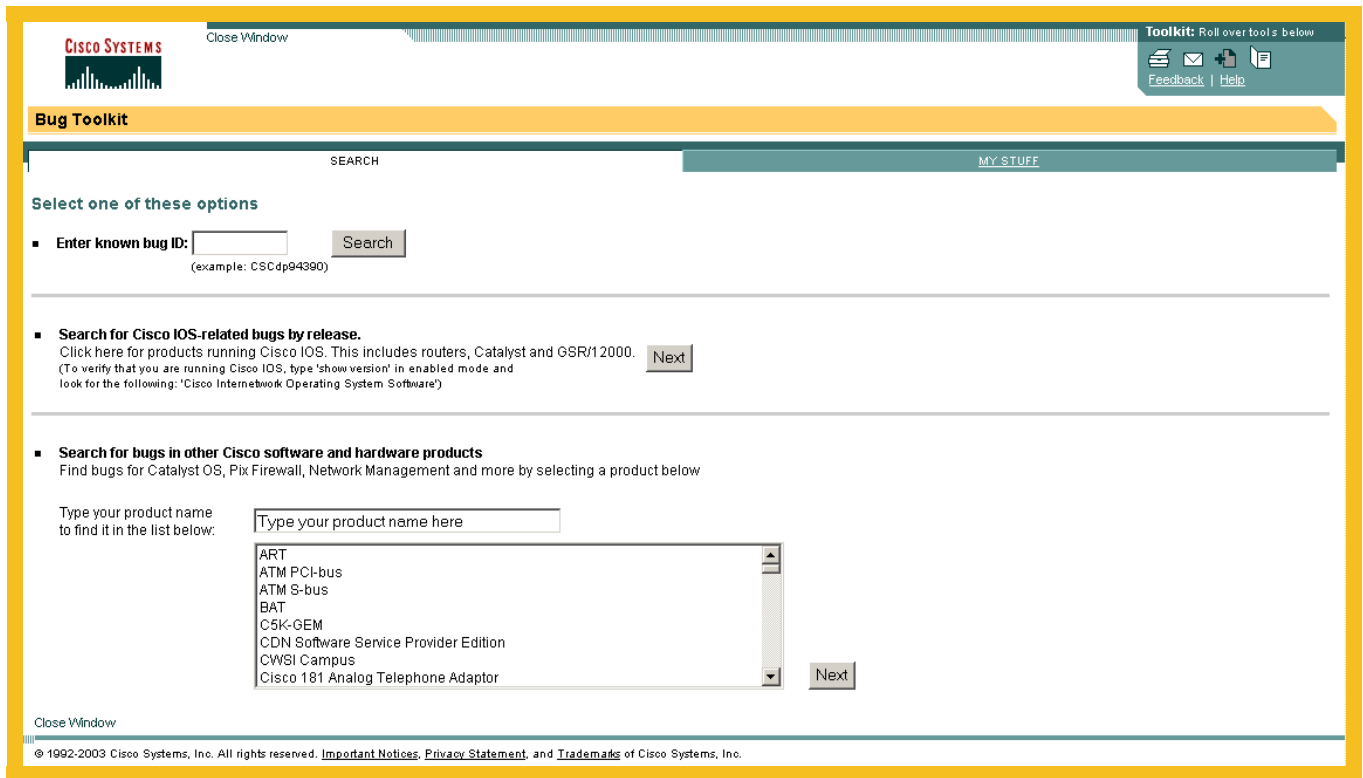
The screenshot shows the Cisco Error Message Decoder web page. At the top, there is a navigation bar with the Cisco Systems logo on the left and links for Home, Logged In, Profile, Contacts & Feedback, Help, and Site Map on the right. Below the navigation bar is a search bar with a dropdown menu set to 'Technical Support' and a 'GO' button. A secondary search bar is located on the right side of the page, with a 'GO' button and a dropdown menu set to 'Search All Cisco.com'. The main content area is titled 'Error Message Decoder' and contains the following text: 'This tool will help you research and resolve error messages for Cisco IOS Software, Catalyst Switches Software, and Cisco Secure PIX Firewall Software. Follow the steps below to receive a description, recommended action, and related resources for your one- or two-line error message. Standard error messages have the following structure : %FACILITY-SEVERITY-MNEMONIC : Message-text (Ex: %SYS-2-MALLOCFAIL). Other console messages (like debugs or router crashes) are not supported by this tool. Please check the [help](#) file for more information. Copy the error message from your device, paste it here, then click Submit.' Below this text is a text input field labeled 'Paste Error Message:' and a 'Submit' button. There is also a checkbox labeled 'suggest related documents within results' which is checked. On the right side of the page, there is a 'Toolkit' section with icons for feedback and help, and a 'Related Tools' section with links for 'TAC Case Open', 'TAC Case Query', and 'Output Interpreter'. At the bottom of the page, there is a footer with links for 'BUSINESS INDUSTRIES & SOLUTIONS', 'NETWORKING SOLUTIONS', 'PRODUCTS & SERVICES', 'TECHNOLOGIES', 'ORDERING', 'TECHNICAL SUPPORT', 'LEARNING & EVENTS', and 'PARTNERS & RESELLERS | ABOUT CISCO'. Below these links are the site navigation links: Home | Logged In | Profile | Contacts & Feedback | Help | Site Map. At the very bottom, there is a copyright notice: © 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

Explanations for console error message strings are listed in the Cisco Software System Messages guide.

<http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl>



### 3 Software Bug Toolkit



The Software Bug Toolkit is a Web-based resource that is used to search for software bugs based on version and feature sets. The toolkit can be used to determine why a feature does not work.

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## 4 IP Subnet Calculator

The screenshot shows the Cisco IP Subnet Calculator web page. At the top left is the Cisco Systems logo. The top navigation bar includes links for Home, Logged In, Profile, Contacts & Feedback, Help, and Site Map. A search bar is located in the top right corner. The main content area is titled "IP Subnet Calculator" and features four tabs: HOME, SUBNETS, SUPERNETS (CIDR), and VLSM. The SUBNETS tab is currently selected. Below the tabs, there is a brief description of the tool's purpose: "This tool provides a way to calculate IP subnetting which is fast, easy, and error free. Choose a function by clicking below or by selecting one of the tabs above." The page then lists three main functions: "Subnets", "Supernet (CIDR)", and "VLSM", each with a short description of what the tool can do for that function. On the right side of the page, there is a "Search" bar, a "Toolkit" section with icons for various tools, and a "Related Tools" section with links to "TAC Case Open", "TAC Case Query", and "2600/3600/3700 Memory Calculator". The footer contains a list of navigation links and copyright information for Cisco Systems, Inc.

IP Subnet Calculator is a Web-based resource that is used to calculate the subnet mask based on several variables. This tool can be used to verify network settings.

<http://www.cisco.com/cgi-bin/Support/IpSubnet/home.pl>

## 5 Password Recovery Procedures

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Tech Notes

# Password Recovery Procedures

**Document ID: 6130**

Please provide your [feedback](#) on this document.

This page is the index of password recovery procedures for Cisco products.

**Note:** For security reasons, the password recovery procedures described here require physical access to the equipment.

### High-End Routers

<a href="#">Cisco 12000 Series Routers</a>	<a href="#">Cisco 7100 Series Routers</a>	<a href="#">Cisco uBR7200</a>	<a href="#">Cisco AGS</a>
<a href="#">Cisco 7000 Series Routers</a>	<a href="#">Cisco uBR7100</a>	<a href="#">Cisco 7500 Series Routers</a>	<a href="#">Route Processor Module</a>
<a href="#">Cisco 7000 Series Route Switch Processor (RSP7000)</a>	<a href="#">Cisco 7200 Series Routers</a>	<a href="#">Cisco uBR10000</a>	

### LAN Switches

<a href="#">EtherSwitch/FastSwitch/FastHub</a>	<a href="#">Catalyst 2100 Series Switches</a>	<a href="#">Catalyst 2950 Series Switches</a>	<a href="#">Catalyst 5500/5000/2926G/2926 Series Switches</a>
<a href="#">Catalyst 1200 Series Switches</a>	<a href="#">Catalyst 2600 Series</a>	<a href="#">Catalyst 3000/3100/3200</a>	<a href="#">Catalyst 6000 Series</a>

This Web page is the source for Cisco password recovery procedures. The password recovery procedure for every Cisco device can be found here.

<http://www.cisco.com/warp/public/474/>

## 6 TAC Case Collection

The screenshot shows the Cisco Technical Support website interface. At the top, there is a navigation bar with the Cisco Systems logo on the left and links for Home, Logged In, Register, Contacts & Feedback, Help, and Site Map on the right. Below the navigation bar is a search bar with a dropdown menu set to 'Technical Support' and a 'GO' button. A secondary search bar is located on the right side of the page, with a 'GO' button and a dropdown menu for 'Search All Cisco.com'. The main content area is titled 'TECHNICAL SUPPORT' and 'TAC Case Collection'. It contains a paragraph describing the tool, a 'Note' about browser support, and several categorized links: ATM Media Support, Dial (Access), Frame Relay, IP Routing Protocols, LAN Switching, Hardware Troubleshooting, Router and IOS Architecture, and Security. Each link is accompanied by a 'NEW!' badge. On the right side of the page, there is a 'Toolkit' section with icons for various tools and a 'Related Tools' section with links to 'TAC Case Open', 'TAC Case Query', and 'Error Message Decoder'.

The TAC Case Collection, is an evolution of the Troubleshooting Assistant tool. It allows users to interactively identify and troubleshoot common problems that involve hardware, configuration, and performance issues. These solutions, which are provided directly by TAC engineers, help resolve networking problems.

[http://www.cisco.com/kobayashi/support/tac/tsa/launch\\_tsa.html](http://www.cisco.com/kobayashi/support/tac/tsa/launch_tsa.html)

## 7 Software Advisor

The screenshot shows the Cisco Software Advisor web application. At the top left is the Cisco Systems logo. Below it is a navigation bar with three tabs: "HOME", "SOFTWARE SUPPORT FOR FEATURES", and "SOFTWARE SUPPORT FOR HARDWARE". The "HOME" tab is currently selected. The main content area contains the following text:

Want to try out what's new in Software Advisor? If you have one of the following supported products:

Switch Series: 4000, 4500, 5000, 5500, 6000, 6500

.... You can [try it now](#).

For each entry point below, you have the option to search for applicable software bugs using the Bug Toolkit.

**Software Support for Features:**

- [Search by Features](#)  
Create your list of Cisco IOS or CatOS features. What software releases support them?
- [Search by Release](#)  
Select your Cisco IOS or CatOS release. Which software features does it support?
- [Compare Releases](#)  
Select two Cisco IOS releases. Which software features are unique to each, and which do they have in common?

**Software Support for Hardware:**

- [Cisco IOS, PIX OS, or WAN Switching Supported Hardware](#)  
Create a list of hardware products. Which minimum software releases are compatible with it?
- [CatOS Supported Hardware](#)  
Populate your Catalyst chassis with CatOS hardware. Which CatOS release will support all the installed hardware?

**Note:** The Catalyst 4000, 5000, and 6000 Series have both Cisco IOS and CatOS supported hardware.

At the bottom of the page, there is a "Close Window" button and a copyright notice: © 1992-2003 Cisco Systems, Inc. All rights reserved. [Important Notices](#), [Privacy Statement](#), and [Trademarks](#) of Cisco Systems, Inc.

The Software Advisor helps users choose the appropriate software for network devices. Users can match software features to Cisco IOS and CatOS releases, compare IOS releases, or find out which software releases support their hardware.

<http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl>

## 8 Feature Navigator II

The screenshot shows the Cisco Feature Navigator II web application. At the top, there is a navigation bar with the Cisco Systems logo, a search bar, and links for Home, Logged In, Profile, Contacts & Feedback, Help, and Site Map. Below the navigation bar, there is a sidebar menu with categories like PRODUCTS & SERVICES, CISCO IOS SOFTWARE, and GENERAL INFORMATION. The main content area is titled "CISCO IOS SOFTWARE" and "Cisco Feature Navigator II". It includes a search bar, a "Toolkit" section with icons for various tools, and a "Related Tools" section with links to Solution Finder for Modular Routers, Dynamic Configuration Tool, Bug Toolkit, and MIB Locator. The main content area also features a section titled "What Took Hours Now Takes Minutes" with a description of the application and several links for searching, comparing releases, and learning about Release 12.3. A small image of a person using a laptop is visible on the right side of the main content area. At the bottom right, there is a prominent blue and white box that reads "CISCO IOS SOFTWARE RELEASE 12.3T".

Cisco Feature Navigator II is a Web-based application that allows users to quickly find the right Cisco IOS Software release for the features they want to run on their networks. Users can search by feature, search by release, or compare two different releases.

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

## 9 TAC Advanced Search

The screenshot shows the Cisco TAC Advanced Search interface. At the top, there's a navigation bar with the Cisco logo and links for Home, Logged In, Register, Contacts & Feedback, Help, and Site Map. Below this is a search bar with a dropdown menu set to 'Technical Support' and a 'GO' button. The main content area is titled 'TAC Advanced Search' and includes a search bar, a 'Look in' section with radio buttons for 'TAC Technical Documentation' and 'TAC Data Collections', a 'Find' section with search criteria like 'with all of the words' and 'with the exact phrase', a 'Type of File' section with radio buttons for document types, and a 'Results per page' section with radio buttons for 10, 25, and 100 results. A 'Search' button is at the bottom. The right sidebar contains 'Search' and 'Toolkit' sections, along with 'Related Tools' and 'Related Links'.

TAC Advanced Search can be used to access the same resources used by TAC. Users can search the entire TAC database for technical documents published by the Cisco TAC, for TAC technical support tools, for documents that are located on <http://www.cisco.com/>, or for entries in the Networking Professionals Connection discussion forums.

[http://www.cisco.com/kobayashi/support/tac/s\\_tac.shtml](http://www.cisco.com/kobayashi/support/tac/s_tac.shtml)

## Appendix B: Instructional Best Practices

### B.1 Definition of Best Practices

#### B.1.1 What is meant by best practices?



**Figure 1: Best Practices**

Since the early 1980s, schools have explored the use of technology as an effective tool for teaching and learning in the classroom. Current research supports certain practices and strategies that help teachers maximize student learning. Instructional concepts such as student centered learning and brain compatible learning have emerged as powerful contributors to advanced student achievement. These types of techniques are referred to as best practices.

The Academy teaching community consists of over 20,000 instructors. Each instructor brings unique experiences and talents to the program. This section presents options that have been successful for certain audiences and certain topics. This section does not imply that all of these techniques apply equally well to all students in all curricula. These techniques, or best practices, form the foundation for effective teaching and learning environments across the Academy curriculum. The Academy program includes CCNA, CCNP, Fundamentals of UNIX, Fundamentals of Voice and Data Cabling, Fundamentals of Java, Fundamentals of Web Design, and IT Essentials.

The ideas presented in this module are taken from international sources such as kindergarten through high school, community colleges, universities, instructional design and training models, and the IT teaching community.



## Web Links

International Society for Technology in Education: <http://www.iste.org/>

Southeast Center for Teaching Quality: <http://www.teachingquality.org/>

Milken Family Foundation: <http://www.mff.org/edtech/>

North Central Regional Educational Laboratory: <http://www.ncrel.org/>

Alabama Best Practices Center: <http://www.bestpracticescenter.org/index.asp>

Mid-Continent Research for Education and Learning: <http://www.mcrel.org/>

## B.1.2 NETS



**Figure 1: NETS Standards**

The International Society for Technology in Education (ISTE) is a nonprofit professional organization that prepares students, teachers, and administrators for a business world that demands proficiency in information technology. The ISTE has written National Educational Technology Standards (NETS) for students, teachers, and administrators. The NETS for Students (NETS•S) are divided into six categories:

- Basic operations and concepts
- Social, ethical, and human issues
- Technology productivity tools
- Technology communication tools
- Technology research tools
- Technology problem-solving and decision-making tools

ISTE also features NETS for Teachers (NETS•T). There are six categories for teacher standards that are based on current research on teaching and learning with technology. The ISTE has considered the need for planning and integration as well as the emergence of new technologies in classrooms. The six categories are as follows:

- Technology operations and concepts

- Planning and designing learning environments and experiences
- Teaching, learning, and curriculum
- Assessment and evaluation
- Productivity and professional practice
- Social, ethical, legal, and human issues

The ISTE has also developed the National Educational Technology Standards for Administrators (NETS•A). Administrators must be prepared to lead the way to systemic reform. Based upon a U.S. consensus, a recognized set of indicators are used within school systems that utilize technology effectively. The following six categories encourage strong leadership in the area of information technology:

- Leadership and vision
- Learning and teaching
- Productivity and professional practice
- Support, management, and operations
- Assessment and evaluation
- Social, legal, and ethical issues

### **Web Links**

ISTE website: <http://www.iste.org/>

### **B.1.3 Literacy, math, and science standards**

Since the late 1980s, states and school districts across the United States have begun to raise standards in core subjects. Academic standards are now used to clearly identify what students should learn and what teachers should teach. State and local standards keep the education system accountable for student achievement.

As state standards have gained momentum, educators have reached an agreement about the meaning of two significant concepts, academic content standards and performance standards, which were later published in the Goals 2000 Act.

Educational standards are important in all countries. The Academy program can be tailored by region, by country, and by curriculum to achieve alignment with international educational standards.

## Web Links

National Council for Teachers of English: <http://www.ncte.org/standards/standards.shtml>

Council for Teachers of Math: <http://www.nctm.org/>

National Science Teachers Association: <http://www.nsta.org/>

American Association for the Advancement of Science: <http://www.aaas.org/>

The National Academy of Science: <http://www.nas.edu/>

National Research Council (NRC): <http://www.nrc-cnrc.gc.ca/>

## B.1.4 TIMSS report

Participating Countries		
Australia	Indonesia	New Zealand
Belgium (Flemish)	Iran, Islamic Republic	Phillippines
Bulgaria	Israel	Romania
Canada	Italy	Russian Federation
Chile	Japan	Singapore
Chinese Taipei	Jordan	Slovak Republic
Cyprus	Korea, Rep. of	Slovenia
Czech Republic	Latvia (LSS)	South Africa
England	Lithuania	Thailand
Finland	Macedonia, Rep. of	Tunisia
Hong Kong, SAR	Malaysia	Turkey
Hungary	Moldova	United States
	Morocco	
	Netherlands	

**Figure 1: TIMSS Report Participating Countries**

The Third International Mathematics and Science Study (TIMSS) indicate how U.S. students perform academically in comparison to students in other countries. The curriculum focuses on trends in math and science achievement. The study completed in 1995 discovers that fourth grade students in the United States scored above the international average. Eighth graders in the United States scored above the international level in science but below the international level in mathematics. Twelfth graders in the United States scored at the lowest possible levels in both math and science.

Two findings emerged when different types of knowledge presentation were compared internationally. First, the United States leads the world in the amount of math and science objectives that are covered within curriculum. However, U.S. students are not taught how to use the information that they are learning. Asian nations and European nations teach fewer objectives and give students more opportunities to use the knowledge in practical applications. This study also finds dissimilarities in teaching styles. In the United States, problem-solving usually occurs after the teacher has demonstrated the process to find the correct answer based upon mathematical principals. Students will then apply this problem-solving process to similar mathematical problems. In countries such as Japan, the order of methodology is reversed. Problem-solving comes first in the sequence of learning. Students are presented with a problem and try to solve the problem based on their current knowledge. They invent their own solutions and then reflect on the process to better understand the mathematical concepts. This study encourages educators to examine teaching practices and content to determine the methods that will lead to higher student achievement.

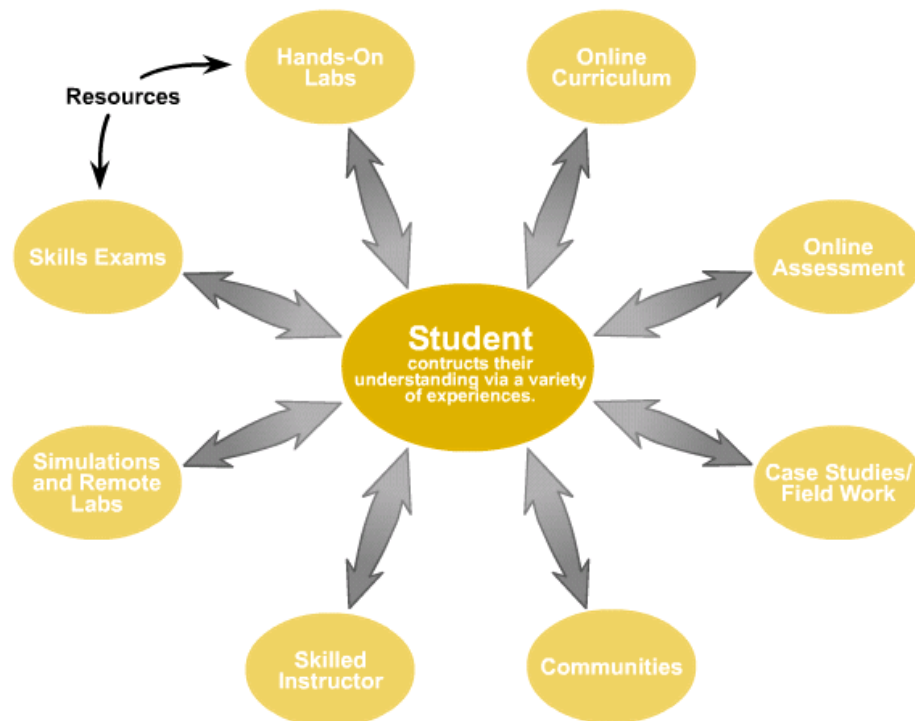
The most recent implementation of this study is TIMSS 1999, which included 38 countries. The 1999 assessment measured the mathematics and science abilities of eighth grade students. Extensive data was collected from students, teachers, and school principals about the mathematics and science curricula. They also investigated instructional practices, home contexts, school characteristics, and policies. The next TIMSS assessment will occur in 2003.

## Web Links

Third International Math and Science Study: <http://isc.bc.edu/timss1999benchmark.html>

TIMSS International Study Center: <http://timss.bc.edu/>

### B.1.5 Student-centered learning



**Figure 1: Learner Model: Academy Student**

Figure 1 illustrates the Cisco Networking Academy learner model. The model is designed to maximize student performance. Instructors are encouraged to strengthen and enhance the online curriculum and labs. When all components of the diagram have been established, research indicates that students are successful in their learning. This model represents a "constructivist learning" approach.

Constructivist learning is derived from the Latin word *constructus*, which means to build. The Cisco Networking Academy allows students to develop knowledge that they can use in the real world. Constructivist learning is also known as student-centered learning. This type of learning is recognized as an exemplary instructional model. This method of teaching puts the students in control of their own learning. It allows them to practice their experimentation, inquiry, problem-solving, decision-making, and communication skills. Constructivist learning can occur on an individual level, in grouped pairs of students, or in small cooperative groups of three or four students.

During constructivist activities, an essential question is presented to individuals or groups of students for thoughts and discussion. Students in a group setting will search for information about issues that surface during their discussion.

Students will also assign roles and identify jobs that need to be completed for the benefit of the group. This allows students to tap into their current knowledge, and journey into new levels of comprehension through a continuous cycle of inquiry and exploration. Students who work individually will go through the same process without any team direction and input. These students will make their own decisions about the relevancy of information. They will rely on their peers and other data sources to determine which information is most useful.

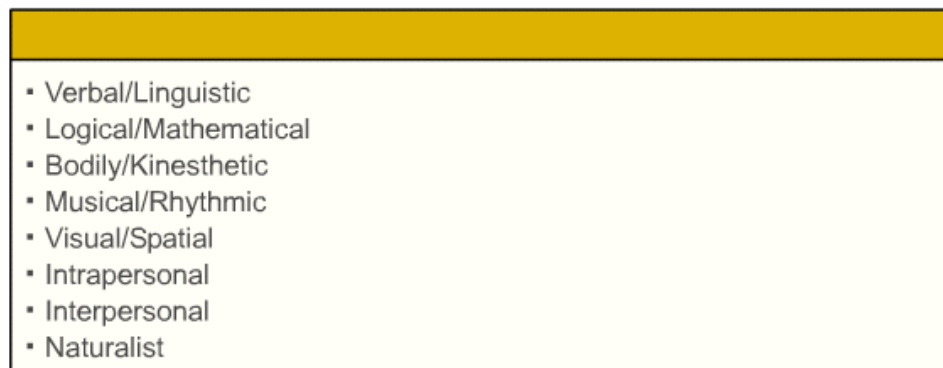
During this time, the teacher will assume a role that is different from the provider of skills and knowledge. The instructor will become a facilitator of learning. As students become immersed in their questions and desire to learn, teachers can ask essential questions to support thinking and exploration. As students struggle with challenges, teachers can introduce problem-solving strategies and encourage students to work through what is perceived to be a difficult situation. As students master the course content, teachers can introduce the next level of challenge.

## Web Links

Pedagogical Application of Technology: A Consortium for Change:

<http://courses.temple.edu/ta/constructivist.htm>

## B.1.6 Multiple intelligences



**Figure 1: Multiple Intelligences**

The research of Howard Gardner provides great insight into how students learn. Students learn in different ways. There are multiple skills that go beyond the traditional verbal and mathematical abilities that are required to master new learning. According to Gardner, there are eight intelligences that people have a predetermined strength to use:

- Verbal/Linguistic intelligence allows students to understand verbal and written forms of words. Students with strong verbal/linguistic intelligence easily recognize sounds, languages, and inflections of speech.
- Logical/Mathematical intelligence allows students to understand and interact with numbers, symbols, and patterns, especially within the disciplines of math and science.

- Bodily/Kinesthetic intelligence gives students a strong connection to new content through the movement and manipulation of body and external objects. Activities help students create cognitive connections for easy recall and comprehension.
- Musical/Rhythmic intelligence centers around melody, tune, pitch, rhythm, and patterns found in types of music or cadence. For some students, music presents an environment that fluctuates from peaceful to highly energetic. Their brains respond accordingly and the recall of new information becomes tied to a specific rhythm or cadence.
- Visual/Spatial intelligence is based on the ability to recognize and respond to visual content through written words or artistic designs. Visual/Spatial strength helps students interpret maps and charts and form mental images of information that is communicated by another person.
- Intrapersonal intelligence provides a confidence in oneself that allows a student to process new information through thought and reflection. Strong intrapersonal intelligence indicates a strong personal connection to feelings and emotions, which can take a student to a higher level of consciousness in learning.
- Interpersonal intelligence allows a student to accurately perceive the emotions, feelings, motivations, and intentions of others. Strong interpersonal intelligence indicates a strong team-player mentality. A student with this strength will work thoughtfully within group settings.
- Naturalist intelligence allows students to recognize natural phenomenon such as flora and fauna, soil and land, weather, and environmental issues. These students easily make choices related to issues such as survival in the wild or the proper clothing for different weather conditions.

Gardner believes that all individuals have strength in one or more of these intelligences and they will follow a changing pattern of strength that depends on their stages of human life and circumstances. For student achievement to be maximized, the Cisco Networking Academy Program encourages instructors to identify the intelligence that best reflects the learning style of individual students.

### **Web Links**

Project Zero: <http://www.pz.harvard.edu/>

## B.1.7 Inquiry-based learning

KWHLAQ
<ol style="list-style-type: none"><li>1. What do we think we <b>K</b>now about the subject?</li><li>2. What do we <b>W</b>ant to find out about the subject?</li><li>3. <b>H</b>ow are we going to go about finding our answers?</li><li>4. What do we anticipate <b>L</b>earning? What have we learned?</li><li>5. Can we <b>A</b>pply our learning to other subjects or projects?</li><li>6. What new <b>Q</b>uestions have surfaced through out time of inquiry?</li></ol>

**Figure 1: Inquiry Based Learning**

When people uncover uncertain, curious, or interesting phenomena in life, questions naturally arise that encourage quests for answers. Inquiry is a natural process that begins as soon as a child starts to experiment with language. As questions are asked, the answers often lead to more questions. This begins a cycle of inquiry for learning. In education, instructors refer to this process as "inquiry-based learning" or "problem-based learning". The basic requirements of either practice are strong reading skills and good scientific observation techniques. One methodology for inquiry-based learning is called KWHLAQ. The following questions breakdown the KWHLAQ method:

- What do learners think they **K**now about the subject?
- What do learners **W**ant to find out about the subject?
- **H**ow are learners going to go about finding the answers?
- What do learners anticipate **L**earning? What have they learned?
- Can learners **A**pply their learning to other subjects or projects?
- What new **Q**uestions have surfaced throughout the time of inquiry?

Within any inquiry-based learning activity or project, the range of control must remain flexible. There will be times when the instructor takes control of the learning environment, times when the students exercise more independence, and times when the instructor and students share control of the direction for learning. The instructor is always a role model for lifelong learning. Teachers show students that even instructors address problems on a daily basis in and out of school. They also model the fact that sometimes problems are solved successfully and other times they are not. Students begin to realize that they will often require a team approach to find the solution to essential questions. In inquiry-based learning, this team consists of the students and the instructor.



## Web Links

Big Rocks and Powerful Kingdoms Personal Learning in Science and Social Studies:

<http://www.ascd.org/readingroom/classlead/9911/2nov99.html>

Using the Internet to Promote Inquiry-based Learning: <http://www.biopoint.com/msla/links.html>

Project Based Learning: What is it?: <http://www.4teachers.org/projectbased/>

### B.1.8 Special needs

Special Needs
<ul style="list-style-type: none"><li>• Visually impaired</li><li>• Hearing impaired</li><li>• Physically impaired</li></ul>

**Figure 1: Special Needs**

When there are visually impaired students in a classroom, here are some general considerations to keep in mind:

- Ask visually impaired students if they need help on specific tasks, but do not assume that they do. The students will ask for help if they need it.
- Use contrasting light and dark colors to help students differentiate between cables and routers.
- Use proper lighting in all areas of the lab to help students see more effectively.
- Provide pocket or lighted magnifiers for reading to assist students with low vision.
- Provide hats or visors to reduce the glare that is associated with many vision disorders.
- Use bold lines and write in large print when information is taught or presented.
- Encourage all students, especially those that are visually impaired, in the classroom. If feelings of hopelessness or fear occur, a social worker or special teacher of the visually impaired may be called in to help these students cope with their learning environment.

When there are hearing impaired students in a classroom, here are some general considerations to keep in mind:

- Make sure the labs are well lighted so the speaker can be clearly seen.

- Be sensitive to background noise in the lab. Turn radios, cell phones, and televisions off during work times. If background noise is unavoidable with online learning, instruct hearing impaired students to use ear phones to keep extraneous noise to a minimum.
- Get close to the students when speaking.
- Stress the importance of only one person talking at a time during group work.
- Initiate conversations with students by specifically calling their names.
- Be patient when students are tired or frustrated with the impact of their disabilities in the lab learning environment.
- Speak face to face. It is important to be on equal eye level with a student when having a conversation.
- Reword sentences or phrases if necessary to convey messages to students who are speech-readers.
- Be conscious of speaking distinctly and not too fast.

When there are physically impaired students in a classroom, here are some general considerations to keep in mind:

- Be prepared to give physically impaired students more time if necessary to complete hands-on labs, tasks, and exams.
- Consider giving these students shorter work assignments with rest periods built into the schedule.
- Establish open communication with the student, parent, and doctor to find the right balance of work that matches individual endurance and capability.
- Configure the lab space to accommodate wheel chairs and other transportation aids.
- Provide preferential seating in the lab to accommodate transportation devices.
- Offer a copy of instructor notes to the student for review on tests.
- Use a computer for testing.
- Provide special devices for students with physical disabilities such as word processors, ergonomically designed furniture, laptop computers, Kurzweil print readers, portable tape recorders for books on tape, and voice synthesis programs.

## Web Links

Disabilities, Teaching Strategies, and Resources: <http://www.as.wvu.edu/~scidis/sitemap.html>

## B.1.9 Learning disabilities

### What are some words commonly associated with learning disabilities?

- **Dyslexia**, perhaps the most commonly known, is primarily used to describe difficulty with language processing and its impact on reading, writing, and spelling.
- **Dysgraphia** involves difficulty with writing. Problems might be seen in the actual motor patterns used in writing. Also characteristic are difficulties with spelling and the formulation of written composition.
- **Dyscalculia** involves difficulty with math skills and impacts math computation. Memory of math facts, concepts of time, money, and musical concepts can also be impacted.
- **Dyspraxia (Apraxia)** is a difficulty with motor planning, and impacts upon a person's ability to coordinate appropriate body movements.
- **Auditory Discrimination** is a key component of efficient language use, and is necessary to "break the code" for reading. It involves being able to perceive the differences between speech sounds, and to sequence these sounds into meaningful words.
- **Visual Perception** is critical to the reading and writing processes as it addresses the ability to notice important details and assign meaning to what is seen.
- **Attention Deficit (Hyperactivity) Disorder (ADD/ADHD)** may co-occur with learning disabilities (incidence estimates vary). Features can include: marked over-activity, distractibility, and/or impulsivity which in turn can interfere with an individual's availability to benefit from instruction.

Figure 1: Learning Disabilities

Instructors will probably have a few students with learning disabilities in their classes. The following list summarizes some approaches to teaching students with learning disabilities. Many of these suggestions also apply to students without learning disabilities:

- Engage the students with lesson starters that illicit emotion and feelings. This introduction to learning instructs the brain to pay attention.
- Provide opportunities for teamwork. Many students with learning disabilities will have a higher level of motivation to succeed in response to peer interactions than when working alone.
- Teach students to write their own personal learning goals. Instruct them to write short and long term goals and provide feedback on their progress.
- Provide numerous models, examples, and representations of curriculum concepts.
- Speak aloud in class to benefit students with learning disabilities. Discuss the steps and thoughts that occur during the problem-solving process.
- Use simple memory tools to help students process information for retrieval at a later time. These tools are called mnemonics and include rhythms or unique patterns of language that are easy to remember. Mnemonics can use pictures, music, color, and movement. This strategy is related to Howard Gardner's work with multiple intelligences.

- Use visual advance organizers to introduce new concepts, analyze, and synthesize levels of comprehension. Organizers prepare the brain for the arrival of new content. This technique builds upon existing knowledge to facilitate the acquisition of new knowledge.
- Use humor, which is a powerful stimulant to the brain. The mind easily latches onto the silly and unimaginable.
- Use movement and action. These are important motivators that can help some students with learning disabilities process information. The hands-on labs will greatly benefit these students.
- Instruct students to talk about or write about what they have learned, what they found interesting, and what they still need to learn at the end of each topic. Reflection moves new knowledge into long-term memory.
- Offer additional time for students with learning disabilities to formulate responses to questions. This extra time can be very important.
- Help students with learning disabilities maintain an emotional state that is free from anger and frustration. Students can work through tasks more easily when they are calm and focused.

### **Web Links**

National Center for Learning Disabilities: <http://www.ncld.org/>

Strategies for Teaching Students with Learning Disabilities:  
<http://www.as.wvu.edu/~scidis/learning.html>

## B.2 Lab-Centric Instruction

### B.2.1 CCNA labs

The CCNA curriculum teaches students how to plan, design, install, operate, and troubleshoot TCP/IP, Ethernet, routed, and switched networks with some remote connectivity.

The CCNA curriculum consists of four courses:

- Networking Basics
- Routers and Routing Basics
- Switching Basics and Intermediate Routing
- WAN Technologies

The curriculum is lab intensive. Approximately 50 percent of all class time is spent on lab exercises.

The required lab equipment for CCNA 1 includes workstations, hubs, switches, a variety of cable making and cable testing tools, and cable installation materials. CCNA 1 students acquire lab skills that enable them to perform the following tasks:

- Configure networking properties on workstations
- Make and test patch cables
- Install and test cable runs, jacks, and patch panels

The required lab equipment for CCNA 2 includes workstations, hubs, switches, and routers. CCNA 2 students acquire lab skills that enable them to perform the following tasks:

- Interconnect networking devices
- Use the Cisco Internet Operating System (IOS) to configure and test routers
- Build and troubleshoot a five-router network

The required lab equipment for CCNA 3 includes workstations, hubs, switches, and routers. CCNA 3 students acquire lab skills that enable them to perform the following tasks:

- Switch configuration
- VLAN configuration
- Intermediate routing protocol implementation
- Use of access control lists to provide traffic control and security on a simple network

The required lab equipment for CCNA 4 includes workstations, hubs, switches, and routers. Optional WAN simulation equipment is also recommended. Students acquire lab skills in the following WAN technology areas:

- PPP
- ISDN
- Frame Relay

Students also must pass a comprehensive lab-skills exam as part of this course.

Standard and premium lab bundles are available. A variety of optional bundles are also available. The student-to-equipment ratio should be as low as possible.

### **Web Links**

Cisco Networking Academy Program: <http://cisco.netacad.net>

## B.2.2 CCNP labs

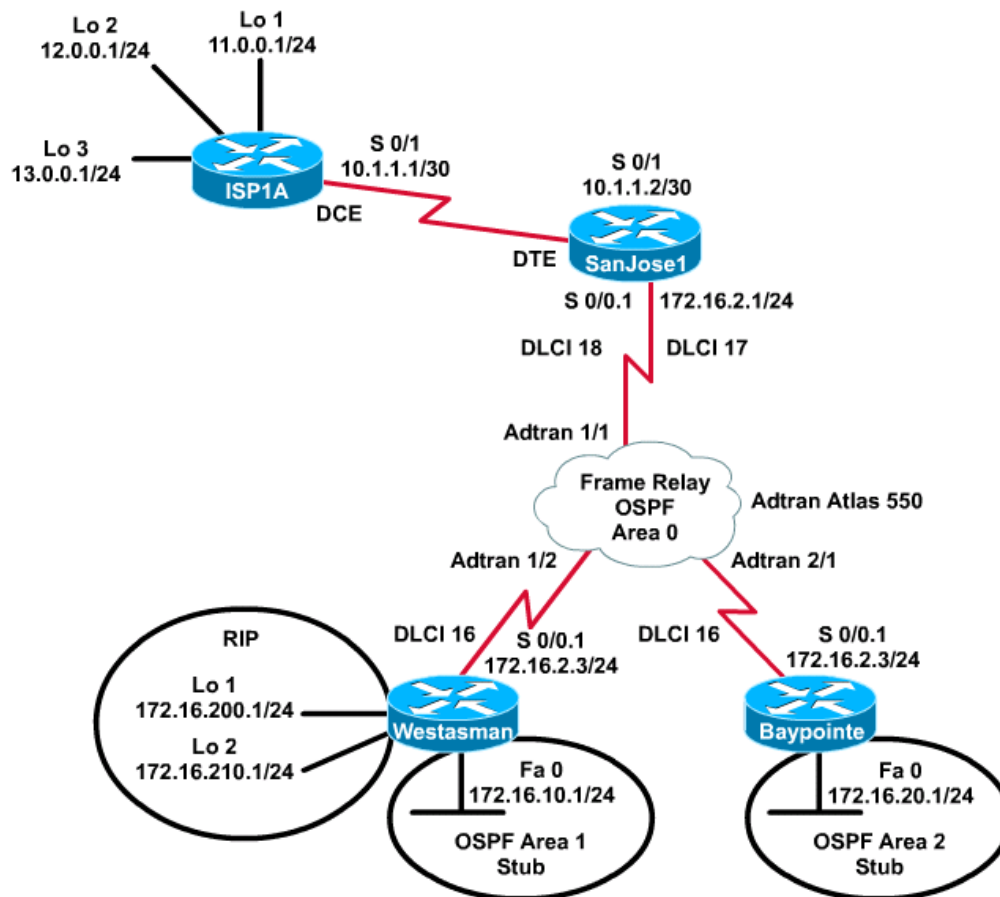


Figure 1: CCNP Labs

The CCNP curriculum teaches students how to plan, design, install, operate, and troubleshoot enterprise-level TCP/IP, Ethernet, routed, and switched networks with substantial remote access.

The CCNP curriculum consists of four courses:

- Advanced Routing
- Remote Access
- Multilayer Switching
- Network Troubleshooting

The curriculum is lab intensive. Approximately 50 percent of all class time spent on lab exercises.

The required lab equipment for CCNP 1 includes workstations, routers, and switches. CCNP 1 students acquire lab skills that enable them to perform the following tasks:

- Design scalable networks

- Implement advanced IP address management techniques
- Configure and test the EIGRP, OSPF, and BGP routing protocols, which help make most enterprise Intranets and the Internet possible

The required lab equipment for CCNP 2 includes workstations, routers, switches, and a WAN simulator. CCNP 2 students acquire lab skills such as the following:

- WAN design
- Dial-up, point-to-point, ISDN, Frame Relay, and X.25 WAN protocol configuration and testing
- Basic network security

The required lab equipment in CCNP 3 includes workstations, hubs, switches, and routers. CCNP 3 students acquire lab skills such as the following:

- Switch and VLAN configuration
- Multilayer switching and redundancy technology implementation
- Campus LAN design

Required lab equipment for CCNP 4 includes workstations, routers, switches, and a WAN simulator. CCNP 4 students acquire lab skills and the ability to troubleshoot the following:

- LANs
- WANs
- Switches
- Routers
- TCP/IP Protocols
- Routing Protocols

Standard and premium lab bundles are available. A variety of optional bundles are also available. The student-to-equipment ratio should be as low as possible.

## **Web Links**

Cisco Networking Academy Program: <http://cisco.netacad.net>



## B.2.3 NETLAB

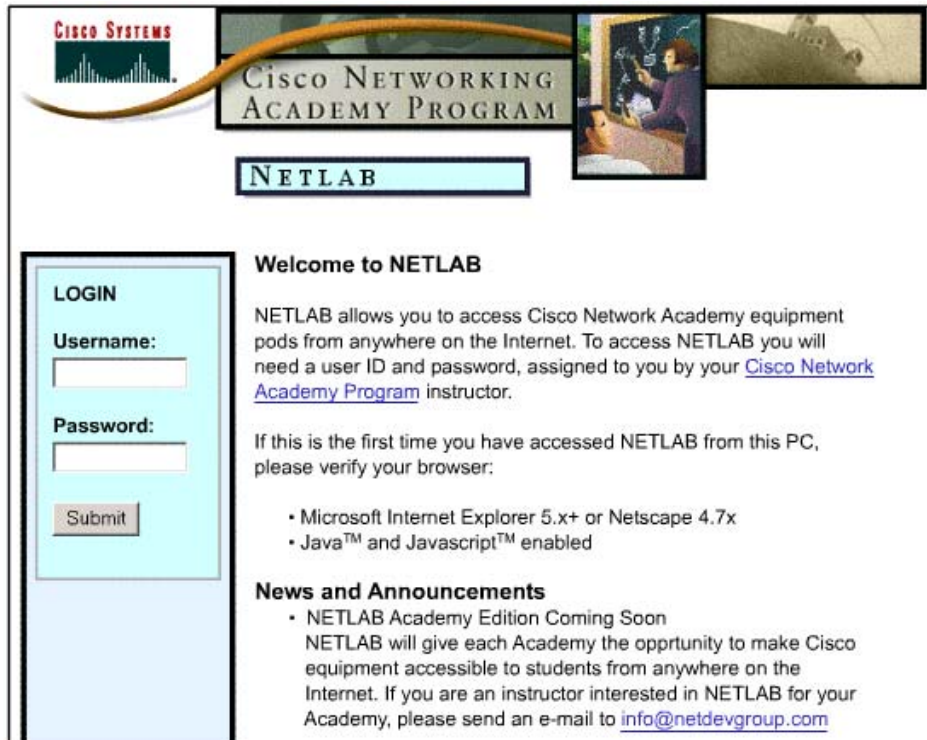


Figure 1: NETLAB

Many educators are interested in remote access to shared lab equipment to give students more access to hands-on experiences. Remote access technologies can be used in courses such as the CCNA, CCNP, and sponsored curriculum to help lower student-to-equipment ratios in distance-learning situations. These technologies are currently fully implemented only for the CCNA courses. This course will examine this issue in more depth and suggest how instructors and Academies can use these technologies or implement their own versions of them.

Cisco Networking Academy now offers the NDG NETLAB solution. This web-based appliance allows Cisco Networking Academies to host live router topologies and curriculum over the Internet. The NETLAB automation and sharing capabilities allow Cisco Networking Academies to maximize the use of their equipment and save money in the process. The networking hardware is identical to the lab bundle used in Cisco Networking Academies worldwide. This will allow students to maintain a consistent topology to practice the configuration commands covered in the Academy curriculum and labs.

The use of NETLAB in the Cisco Networking Academy will allow students to log in, create, and edit configuration files. Students can also program one or more of the devices. Students can work in teams to configure an entire topology or schedule individual time to practice new commands. Since the NETLAB environment equipment is similar to the equipment used by Cisco Networking Academy programs, students can practice configuration tasks just as they would with their Networking Academy equipment. Since the NETLAB equipment can be accessed from any PC with a browser that is connected to the Internet, students can perform these configuration tasks outside of the Academy.

Students will usually access the equipment in the evening or on the weekends from their homes or another location with Internet access. Some instructors may choose to implement use of the NETLAB system within the classroom. This is especially useful when students are just beginning to learn new configuration tasks.

Instructors can use the instructor-led lab features of NETLAB to lead the class through a lab. During instructor-led sessions, the instructor can issue configuration commands to one or more devices while students shadow the Telnet session of the instructor. Another way instructors can use NETLAB within the classroom is the team approach. A team of students is given an assignment to configure one or more of the routers in a topology. The team can use NETLAB to share access and control over the routers while other teams try to configure other routers in the topology. Since NETLAB can save and store these configuration files, it is easy for the instructor to evaluate the performance of each team.

NETLAB has also been used by instructors to review the work of students on real equipment. During each lab reservation, NETLAB records every command and router output in log files. The final equipment configurations of students can be saved for instructor review. This feature allows instructors to determine the ability of students to implement the concepts learned in the classroom. Instructors can also identify and correct common mistakes that are made by students during lab exercises.

NETLAB is currently deployed as a pilot program at selected Cisco Networking Academies. Upon the successful completion of this pilot program, Cisco will offer NETLAB to all Cisco Networking Academies. For information on how to become one of the Academies that participates in the NETLAB project pilot, please e-mail [netlab-pilot@cisco.com](mailto:netlab-pilot@cisco.com). Interested Academies will receive a survey that will help identify any changes that will need to be made for the NETLAB tool to function and information on how to order the necessary equipment. Please e-mail [netlab-question@cisco.com](mailto:netlab-question@cisco.com) with any questions or requests for additional information. This process is designed to minimize potential deployment problems and to enhance the success of a production deployment. Academies will be selected for this program based upon a review of several factors. Technical capacity will be one of the more important criteria. A survey will be provided to interested Academies to identify the requirements for a successful solution. Academies will need to have the proper infrastructure in place and must be able to demonstrate a sufficiently high level of technical expertise.

To learn how to utilize NETLAB, the Cisco Networking Academy Program has created an online curriculum and comprehensive administrator, instructor and student guides. Although NETLAB seems intuitive and easy to use, administrators and instructors should spend time becoming familiar with the numerous features of NETLAB.

## Web Links

NGD NETLAB: <http://www.netdevgroup.com/netlab.htm>

## B.2.4 Simulations

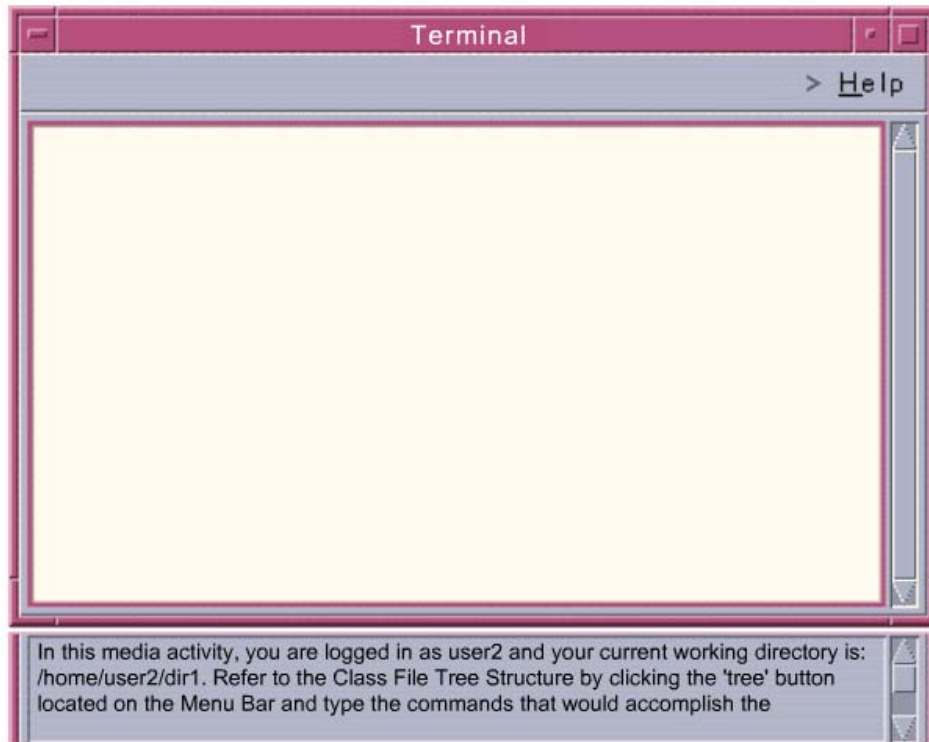


Figure 1: Simulations

Research indicates that learning is more extensive when content is interactive and provides instant feedback. The Academy curriculum contains a variety of interactive Flash activities. One class of these activities is simulation. Examples of simulations are content items, such as, command-line interfaces (CLIs), graphical user interfaces (GUIs), and programming language development environments.

Figure 1 shows a simulation activity from the UNIX curriculum. The Help feature in the simulation can be used to obtain the necessary information to complete the required task.

There are generally three levels of Academy simulations:

- **Syntax drill** – The simplest and most scripted activity can be thought of as a syntax drill. This exercise gives students immediate practice when a new command or procedure is introduced. These simulations help move online curriculum away from an e-reading approach to a more interactive e-learning approach.
- **Lab drill** – The second level can be thought of as a lab drill. This exercise involves a step-by-step simulation of hands-on labs and configuration tasks. The hands-on lab or configuration task will include a complete flash analogue that can be done by students even if they have no access to the lab equipment.

- **Simulation** – The third level is called simulation. This is the most open-ended environment. This level is not scripted. Therefore, it supports a wide variety of hardware and software behavior. For command-line interfaces such as IOS or UNIX, many commands can be issued in any order. The best example of this third level simulation environment is eSIM, which is available and free to all CCNA and CCNP students.

Flash simulations are meant to complement hands-on experience with lab equipment and actual programming. These simulations have many cognitive benefits. For example, simulations allow students to perform a simulative lab activity prior to an actual lab activity. This helps students increase their level of comprehension in a simulated environment before they are required to demonstrate a final proficiency with equipment and programming. In the future, many more simulations across the curricula will be developed for the Cisco Networking Academy Program.

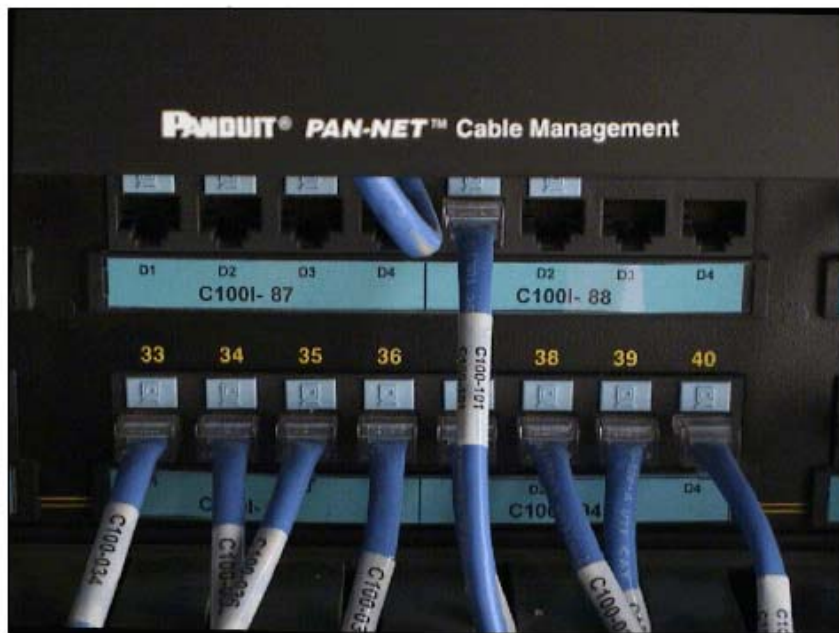
### B.2.5 Sponsored curriculum labs



---

IT Essentials I and II: Sponsored by Hewlett-Packard

**Figure 1: Sponsored Curriculum Labs**



---

Fundamentals of Voice and Data Cabling: Sponsored by Panduit

**Figure 2: Sponsored Curriculum Labs**



---

Fundamentals of UNIX: Sponsored by Sun Microsystems

**Figure 3: Sponsored Curriculum Labs**

The six sponsored curricula also require dedicated labs and a variety of hardware and software. They are summarized in the following sections:

### **IT Essentials: PC Hardware and Software IT Essentials** <sup>1</sup>

PC Hardware and Software, which is sponsored by Hewlett-Packard Company, presents an in-depth exposure to computer hardware and operating systems. Students learn the functionality of hardware and software components and the suggested best practices for maintenance and safety issues. Students learn how to assemble and configure computers, install operating systems and software, and troubleshoot hardware and software problems through hands-on activities and labs. An introduction to networking is also included. This course helps students prepare for the CompTIA A+ certification exam. This is designed as a 70-hour course. However, it addresses a broad range of topics that might benefit from a longer delivery model.

### **IT Essentials: Network Operating Systems** <sup>1</sup>

Network Operating Systems, which is sponsored by Hewlett-Packard Company, is an extensive introduction to multiuser, multitasking network operating systems (NOSs). This course will discuss the characteristics of the Linux, Windows 2000, NT, and XP NOSs. Hands-on labs will utilize the Windows 2000 and Linux NOSs. Students will explore a variety of topics such as installation procedures, security issues, back up procedures, and remote access. This is a 70-hour course.

### **Fundamentals of Voice and Data Cabling** <sup>2</sup>

Fundamentals of Voice and Data Cabling, which is sponsored by Panduit, is designed for students interested in the physical aspects of voice and data network cabling and installation. The course focuses on cabling issues related to data and voice connections and discusses the industry and worldwide standards, types of media and cabling, physical and logical networks, and signal transmission. Students will develop skills in the following areas:

- How to read network design documentation
- Part list set up and purchase
- How to pull and mount cable
- Cable management
- How to choose wiring closets
- Patch panel installation
- Termination
- Jack installation and cable testing

This is a hands-on, lab-oriented, 70-hour course. It stresses the following competencies:

- Documentation
- Design
- Installation issues

- Laboratory safety
- On-the-job safety
- Working effectively in group environments

### **Fundamentals of UNIX** <sup>3</sup>

Fundamentals of UNIX, which is sponsored by Sun Microsystems, provides students with the following:

- Ability to use UNIX operating system commands
- Hands-on experience with basic Sun Microsystems Solaris™ operating environment commands
- Introduction to the Common Desktop Environment (CDE), which is the graphical interface between different environments

This class is intended for new users of UNIX. Students will learn the fundamental command-line features of the Solaris environment:

- File system navigation
- File permissions
- The vi text editor
- Command shells
- Basic network use

CDE features include standard desktop tools, text editor, printing, and mail. The course is designed for 70 hours. About half of this time is spent on the instructor-facilitated online multimedia material and the rest is spent on lab exercises.

### **Fundamentals of Java Programming**

Fundamentals of Java Programming, which is sponsored by Sun Microsystems, provides a conceptual comprehension of Object Oriented programming. The course also teaches students how to use the JAVA language object oriented technologies to solve business problems. Topics include the language fundamentals and the Java language application programming interface (API). Students will learn how to use this language to create classes, objects, and applications. This course also addresses the demand for training and preparation to be a Sun Certified Programmer for Java™ 2 Platform. This is designed as a 70-hour course. However, it addresses some very advanced topics that might benefit from a longer delivery model or some pre-selection and screening of students.

### **Fundamentals of Web Design**

Fundamentals of Web Design, which is sponsored by Adobe Systems, will focus on the overall production processes related to website design. The emphasis of the course will be on design elements that involve layout, navigation, and interactivity. Cisco Networking Academy students will learn Web design in preparation for higher education or jobs in the Internet economy. Hands-on Web design exercises will use Adobe® Photoshop®, Adobe Illustrator®, Adobe GoLive™, Adobe LiveMotion™, and Adobe Premiere®. This course has been designed as a 70-hour course. However, since it uses five Adobe applications, it may be beneficial to use a

longer delivery model or some pre-selection and screening of students. About half of the course time is spent on the instructor-facilitated online multimedia material and the rest is spent on lab exercises.

### **Web Links**

Instructor Community: New Courses:

[http://cisco.netacad.net/cnacs/prot-doc/new\\_courses.html](http://cisco.netacad.net/cnacs/prot-doc/new_courses.html)



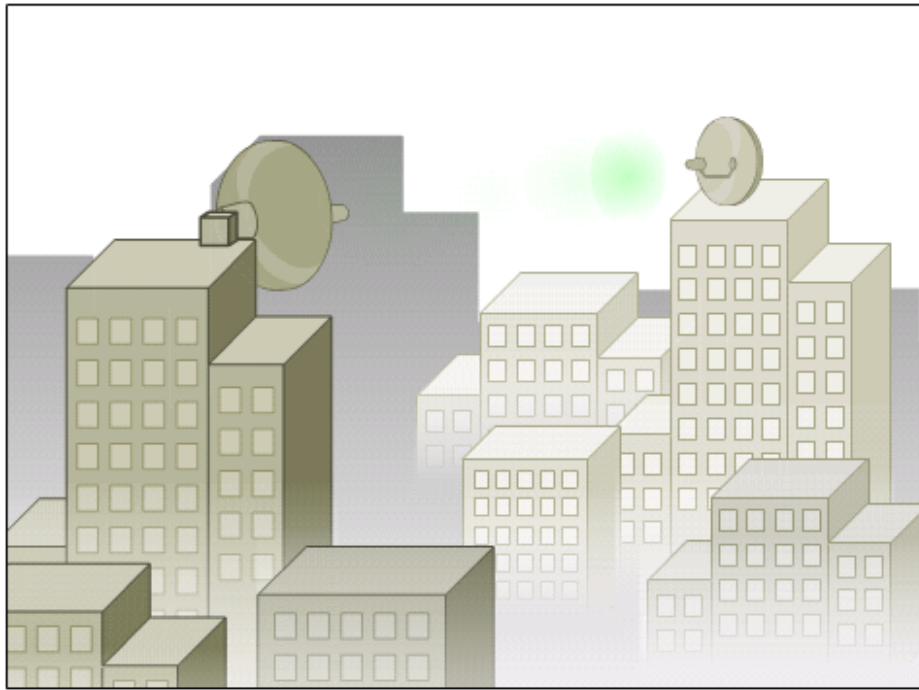
## B.2.6 Emerging technologies



Figure 1: PIX Firewall PhotoZoom



Figure 2: IP Phone



**Figure 3: Wireless LAN**

In the future, new technologies such as network security, IP telephony, and wireless LANs may be the basis for Academy courses.

Each of these courses will have an associated lab bundle, which will allow for the successful implementation of the labs. The goal of these course will be to train professionals who can implement network security [1], IP telephony [2], wireless LANs [3], and other networking technologies.

### **Web Links**

Network security issues: <http://cisco.com/warp/public/779/largeent/issues/security/>

IP Telephony:

<http://www.cisco.com/warp/public/779/largeent/learn/technologies/IPtelephony.html>

Wireless solutions:

<http://www.cisco.com/warp/public/779/smbiz/netsolutions/find/wireless.shtml>

## B.2.7 Troubleshooting

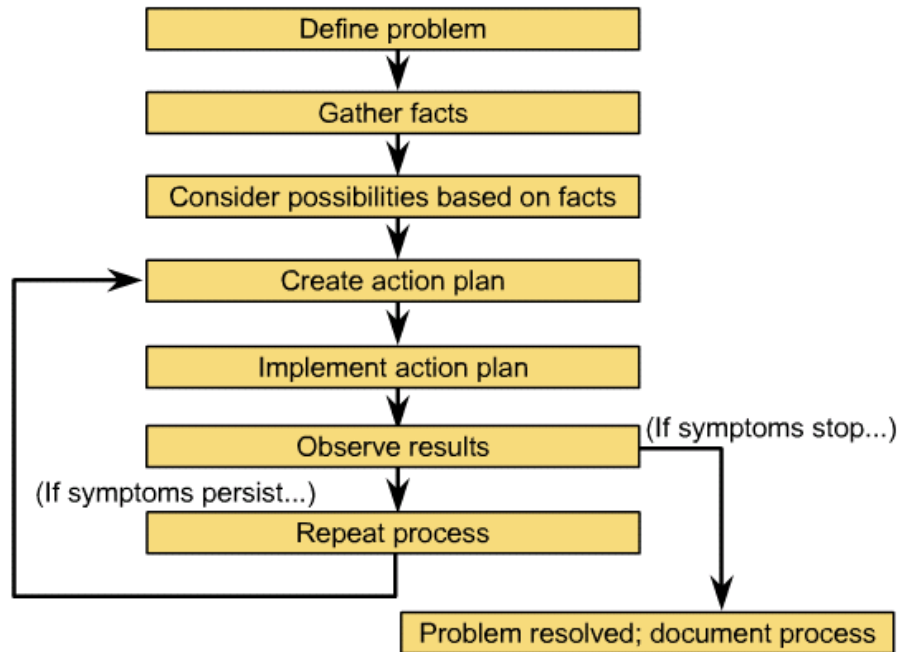


Figure 1: Steps in the Problem-Solving Model

Troubleshooting is a form of educational inquiry that is necessary in most Academy courses, even if it is not formally taught.

There are literally over a hundred approaches to troubleshooting. Figure 1 shows one approach. This is the preferred method for Cisco courses. Instructors may use their own preferred method.

Troubleshooting and debugging skills are necessary for students who seek further education and employment in the IT industry. Instructors will typically need to spend more time on lab preparation to teach students about troubleshooting. However, the overall benefit to the student is worth this investment. Troubleshooting is used to identify and correct hardware, software, and programming problems.

One instructional troubleshooting method involves deliberately introducing a finite number of problems, in a structured lab environment, that have been experienced previously by the students.

With practice, students will be able to diagnose and fix the problems in a finite amount of time. This method must be integrated with labs that do the following:

- Expose students to a working system
- Demonstrate the typical failure modes of that system
- Allow students to experience first hand the symptoms of those failure modes

- Provide opportunities for students to practice diagnosis and repair

### **Web Links**

Teaching Methods Web Resources:

<http://www.mhhe.com/socscience/education/methods/resources.html>

The Universal Troubleshooting Process (UTP): <http://www.troubleshooters.com/tuni.htm>

Journal of Technology Education: <http://scholar.lib.vt.edu/ejournals/JTE/v2n2/html/deluca.html>

## B.3 Project-based Instruction

### B.3.1 Challenges and projects

#### NetDay Hero Awards

Each year, NetDay recognizes outstanding individuals who, through their heroic and selfless leadership, have made significant contributions to education and education technology. This award, the NetDay Hero Award, honors individuals who have made a life-long commitment to improving and enhancing educational opportunities for children through the use of technology. 2002 Hero Award Recipients: Elaine and John Chambers



We are proud to honor Elaine and John Chambers as the 2002 NetDay Heroes in recognition of their extraordinary leadership and vision in both their professional and family commitments to education and education technology. The Chambers' have a long-standing history of supporting education as individual philanthropists and corporate citizens. As CEO of Cisco Systems, Inc., John has positioned Cisco's educational programs to represent powerful partnership models for corporations, schools, and nonprofits to achieve results in education.

Elaine and John Chambers received their 2002 Hero Awards at NetDay's annual Family Celebration on March 9, 2002 at The TECH Museum of Innovation in San Jose, CA.

Source: <http://www.netday.org/>

Figure 1: Challenges and Projects

NetDay challenges are problem-based labs or projects that are advocated by AAAS Project 2061, which is a science education reform project. Unlike step-by-step labs, these exercises encourage students to develop their own solutions to various problems or challenges. The challenges vary in content and duration ranges from 50 minutes to 3 weeks. These challenges consist of two basic parts. First, the lab asks students to solve a problem. Second, it asks the students to create a product. For example, a simple 50-minute challenge lab for the first semester might be titled "Make a Patch Cable that Works Successfully". A three-week challenge that teaches more complex tasks might be called "Wire the School Computer Lab". NetDay is a great example of challenge-based learning, and Cisco encourages instructors to incorporate it into their classes.

Teaching and learning environments extend beyond the lab setting. Opportunities for real-world applications emerge when students can use their networking skills in projects that contribute to community initiatives. Sometimes these activities are called service learning.

The Cisco Networking Academy Program originated as a community project. In the mid-1990s, educational institutions around the world experienced a demand for computer networks that exceeded the skilled personnel available to install and maintain those networks. Cisco engineer George Ward worked to address these issues. He articulated the need for a course sequence that would train high school students to support their school networks. This need for versatile apprentices became the Cisco Certified Network Associate (CCNA) curriculum.

A NetDay occurs when a community volunteers time to wire a school. It is a popular type of community project that involves students, parents, network administrators, and others who work together to get students connected to the Internet. Academy students participate in numerous NetDays.

Another example of a community project was developed by the Cisco Academy of South West Ohio (CASWO). This Academy and its students provided technical support for the annual Ohio SchoolNet Technology Conference. Academy students helped set up the network for the conference and provided technical assistance to conference managers and presenters. One quote from a student demonstrates the value of this learning experience, "This really helped me see the big picture of how everything works together and what tech support is like".

Another example of community outreach takes place in Washington, D.C. where Cisco Systems partners with Mary's Center for Maternal and Child Care. With help from a volunteer system engineer and three students from the Cisco Networking Academy Program at Bell Multicultural High School, Mary's Center now has a fully operational wireless network that can support their computer needs. Now the center can access important health and insurance information needed to assist families and their children. Academy students receive many benefits from working on real-world projects. These benefits are described in a quote from Max Anis, a Networking Academy instructor at Bell High School, "These students return to the classroom with an incredible amount of energy after these experiences. As a result, they are even more determined to complete the program and continue their pursuit of a career in the industry".

## B.3.2 Design activities

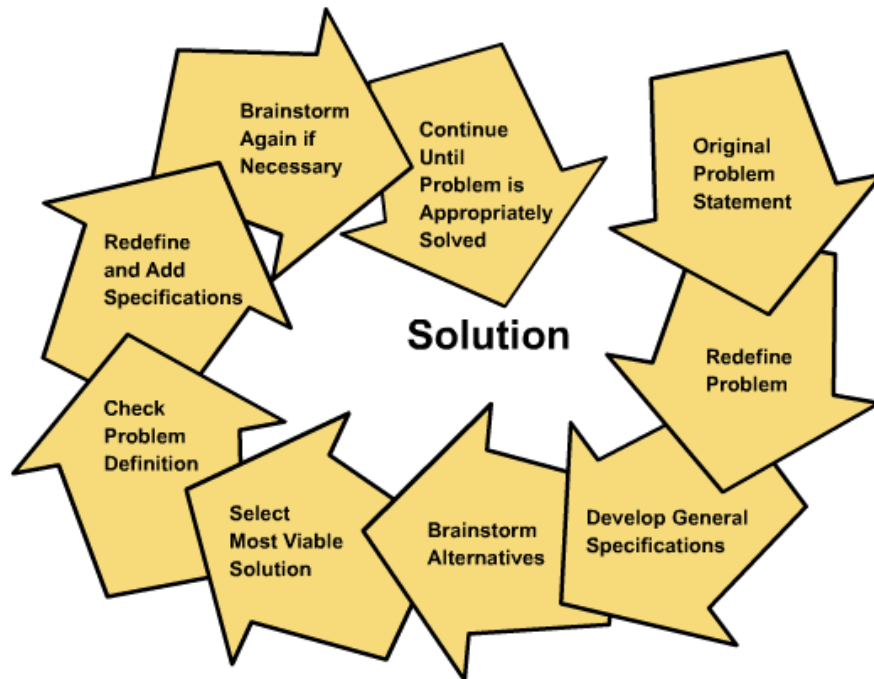


Figure 1: Dartmouth Problem-Solving Cycle

Design is an iterative process that starts with brainstorming. From there, it proceeds through research and problem-solving matrices and design specification tests. Multiple repetitions of this process are required until an adequate solution to a problem is achieved. Any Academy curriculum with projects or design activities allows instructors to introduce elements of the Dartmouth Problem-Solving and Design Method. The website associated with this section has online resources and written materials that can be downloaded and a video that can be ordered. There are other methods that are also effective. Cisco encourages instructors to use the method that works best for them and their students.

Whether students will troubleshoot problems in an existing network or design and check a network to meet specifications, the process involves an iterative problem-solving procedure. For Internet problems and issues related to general engineering, problem-solving matrices are useful when there many alternatives for a given number of constraints. Chapter 1, The Engineering Problem-Solving Cycle of the Engineering Problem Solving for Mathematics, Science, and Technology Education, uses the problem solving matrix to introduce the problem solving cycle and its iterative nature. The matrix teaches students how to define a problem. Chapter 4, Guiding Students Through the Problem-Solving Cycle, explains how the entire process can be iterated. This includes suggestions on how to choose effective problems, how to set up the right environment for brainstorming sessions, and how to analyze the results of these sessions.

The goal is for students to gain an appreciation for the importance of problem solving, which is one of the most important aspects of engineering. Cisco also wants students to experience the use of these procedures to gain a better comprehension of why some potential solutions work and others do not. They will learn that the ability to employ good problem-solving procedures and documentation will ultimately determine their success with problem solving. Eventually,

students will be able to use the lessons learned from failed problem-solving attempts to save time when they try to solve new problems. Chapter 5, Research, Documentation, and Testing, is a good resource for students to learn how to conduct site surveys, keep work logs, produce engineering reports, and create portfolios.

### **Web Links**

Dartmouth Problem-Solving and Design Method: <http://thayer.dartmouth.edu/teps/index.html>



### B.3.3 Brainstorming

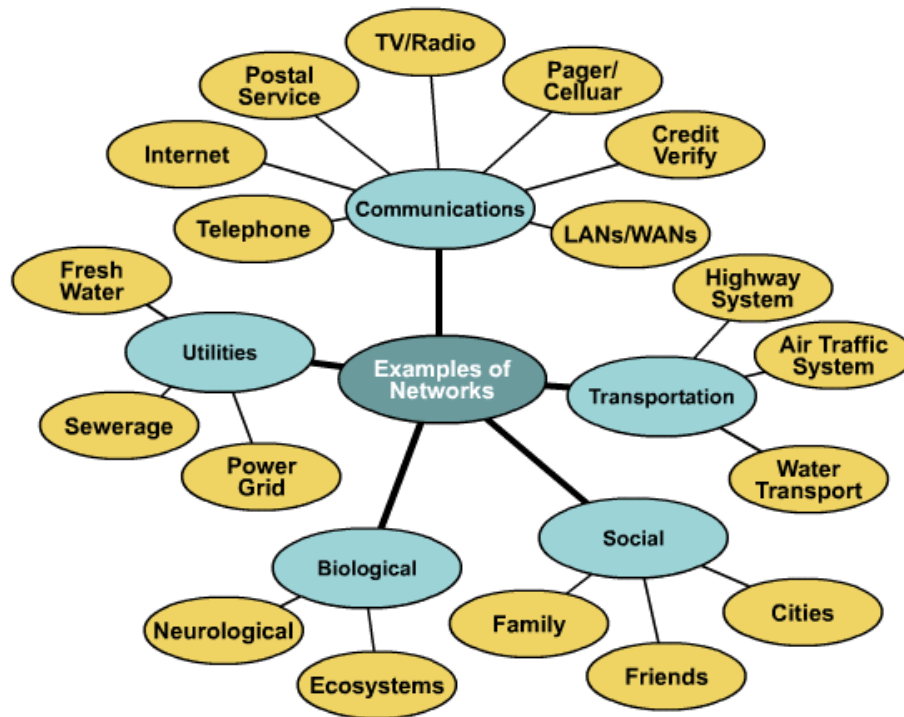


Figure 1: Cluster Diagram

Brainstorming techniques can be useful for teaching IT curriculum. These techniques can be applied to areas such as introductions to new topics and integral parts of design work, Figure 1 shows some responses to the question, "What does the word 'network' mean?" There are four simple rules for this brainstorming activity:

- The wildest possible ideas are accepted.
- There will be no censorship of ideas.
- The instructor wants a high quantity of responses.
- Responses can build on the ideas of other people.

Another method for brainstorming is called carousel brainstorming. This is a strategy used for creative thinking when multiple solutions are possible to solve an issue or problem. During a carousel session, problems are documented on large sheets of chart paper around a room. Students in small cooperative groups are given different colored pens and asked to go around the room and brainstorm solutions to the problems listed on the different chart papers. This is done in 30-second rotation sessions. The process continues until students have an opportunity to respond to all problems or issues listed on papers around the room.

SCAMPER is another example of a brainstorming activity that encourages students to think creatively. Scamper is an acronym for substitute, combine, adapt, modify, put to other uses, eliminate, and reverse. It was first implemented in the 1940s by Alex Osborne and it was revised in the early 1980s by Bob Eberle.

SCAMPER involves a series of questions related to a new process or concept. After students encounter new information, they respond to the following questions:

- **Substitute** – What material, methods, processes, or situations can be used in place of this?
- **Combine** – What materials, methods, processes, or situations can be combined or added to influence this issue or problem?
- **Adapt** – Can the materials, methods, processes, or situations be used in another way to find a solution?
- **Modify** – Can this be made bigger, stronger, and more frequent? Can it be made smaller and more compact?
- **Put to other uses** – Can this be used instead of other materials, methods, processes, or situations?
- **Eliminate** – Can parts of this be eliminated?
- **Reverse** – Can the work be done backwards? Can this process be reversed?

SCAMPER emphasizes that no response is too crazy or inconceivable.

### Web Links

Gifted Education - A Resource Guide for Teachers:

<http://www.bced.gov.bc.ca/specialed/gifted/process.htm>

Scamper: <http://www.discover.tased.edu.au/english/scamper.htm>

### B.3.4 Case studies

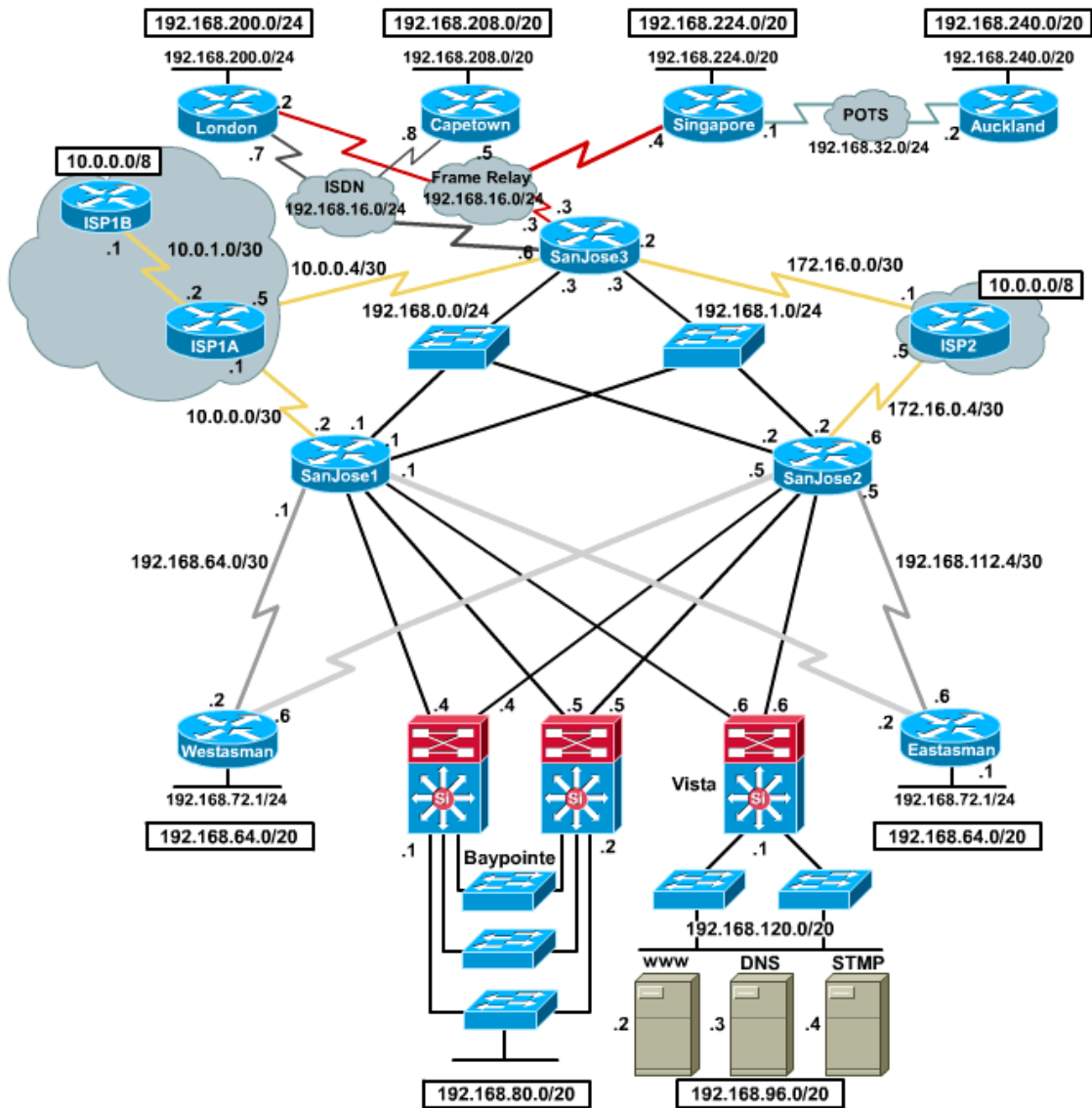


Figure 1: Case Studies

Case study teaching methods have become more important in many professions such as law, medicine, and business. Case studies that are specified in the course or instructor-developed can be used to integrate many concepts throughout the Academy curricula.

Figure 1 shows a case study from the CCNP curriculum. The International Travel Agency is a fictitious business for which a CCNP certified individual might be asked to provide network services.

## Web Links

Use of Master Classroom Technology to Implement a Case Study Approach to Learning:

<http://www.mtsu.edu/~itconf/papers96/MASTER.HTM>

Case Study Teaching in Science: A Bibliography:

<http://ublib.buffalo.edu/libraries/projects/cases/article2.htm>

## B.3.5 Web research

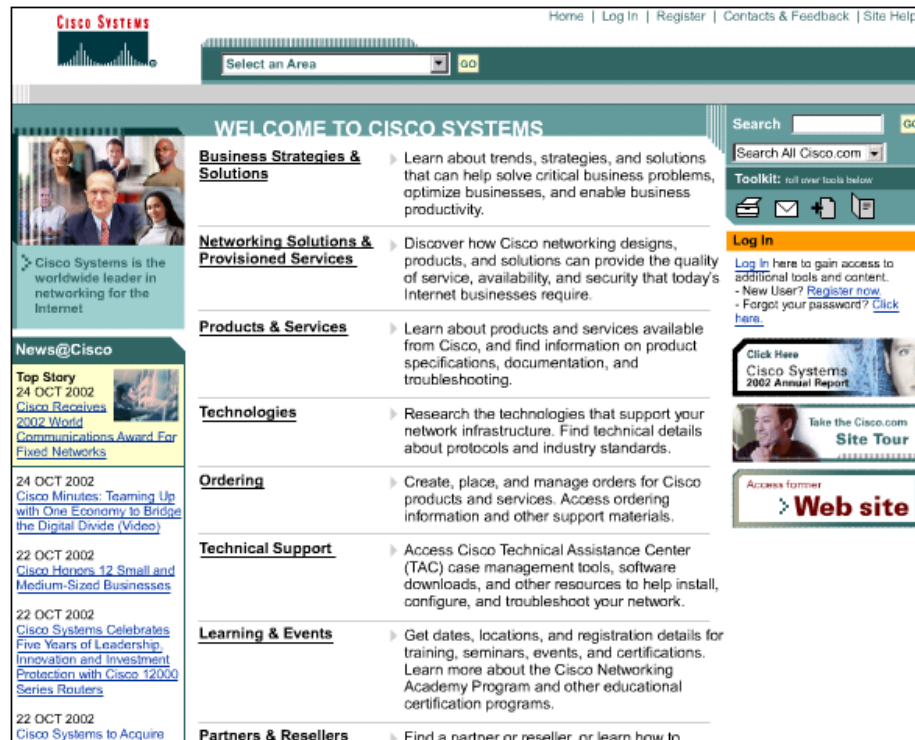


Figure 1: Cisco.com

The Internet has a tremendous amount of resources for people who want to understand or install networks. Students can also research products, answer questions, or perform extension activities. Academy students are encouraged to use the links built into the Instructors Guide or their favorite websites. The online documentation for Cisco Systems, Sun Microsystems, HP, Panduit, and other sponsors is particularly important. In terms of bandwidth capabilities, the Web resources related to networking far exceed any textbook or online curriculum. Students must find the resources and be cautious consumers. The ability to use the Internet as a resource is a very useful skill for students to develop.

### Web Links

Cisco: <http://www.cisco.com/>

Sun: <http://www.sun.com/index.xml>

Adobe: <http://www.adobe.com/>

Panduit: <http://www.panduit.com/>

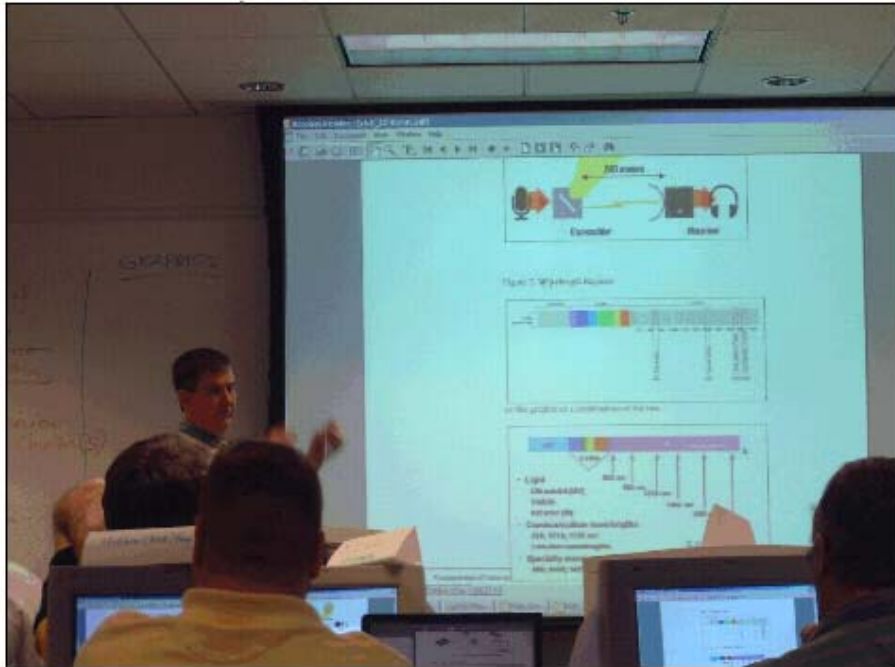
Hewlett Packard: <http://www.hp.com/>

Google: <http://www.google.com/>

Yahoo: <http://www.yahoo.com/>

## B.4 Instructional Strategies

### B.4.1 Instructor-led classrooms



**Figure 1: Instructor-Led Classrooms**

The instructor-led style of instruction is currently the most commonly used approach. Academy instructors must communicate information to students based on required competencies and performance objectives. Instructor-led environments allow instructors to cover specified subject matter with a large group or small group of students at the same time. This style of instruction can take place in an extended time frame, which might require an entire class period, or in a shorter time frame as a mini-lecture. Mini-lectures focus on smaller chunks of content that students may need to hear at some point in the learning process. An effective classroom strategy for this style of instruction is to present all lectures at a predetermined class time, and as a precursor to individual and group work. The current focus on the cooperative dynamics of learning has taken attention away from the importance of knowledge-based processes and procedures. Within the instructor-led environment, teachers can review strategies that will help students become better listeners. This will prepare them to be more effective communicators in the academic and working world.

- A mini-lecture is a 10-minute lecture format that might consist of the following elements:
- A hook
- A pretest or focus question to test for comprehension
- The actual lecture
- A short question or activity

Studies have found that relatively short, engaging lectures that include demonstrations are excellent adjuncts to the online curriculum and lab activities.

## B.4.2 Self-paced instruction

Academy courses implement self-paced instruction and learning strategies. In self-paced instruction, students learn new content at a speed of comprehension that best fits their learning style. The content is presented in modules, which are chunks of information that fit together into a comprehensive whole. Modules are effective because they allow students to acquire new knowledge in manageable pieces. This method of teaching and learning is used in online environments. Self-paced instruction in an online environment allows students to journey through new competencies or knowledge with flexible time and space requirements.

The purpose of online learning should be stated early in the course so students understand what objectives and performances they will be required to master during a course experience. As they begin their voyage into new content, students will encounter linked resources through the Internet and other electronic connections. Through exploration and experimentation, online learning will allow students to become actively involved with the content. Curiosity and inquiry will drive student interest. Self-paced instruction will provide the path to their success. In any online or self-paced program, there is a strong need for a course facilitator. This person helps get students excited and keeps them excited about what they are learning. This person also monitors student progress.

The online lessons are an important part of Academy instruction. However, they should not be overly used. Remember that a primary goal of the Cisco Networking Academy Program is to train students to design, install, and maintain networks. This is fundamentally a hands-on, lab-based endeavor. When the online curriculum is used in a classroom, students should view the content individually or in pairs of two while the instructor circulates throughout the room to check for problems and comprehension. Instructors may periodically interrupt students to provide additional information or clarify content.

Study Guides provide an organized method for students to record the important concepts of each lesson. These can be used for review and reflection.

Self-paced instruction includes the following components:

- **Learn** – Knowledge is gained through vocabulary, content, and activities.
- **Vocabulary** – Students use the glossary to list and define new terms.
- **Notes or Ideas** – Important information from the lesson is recorded.
- **Activity** – Students complete the activity assigned in class.
- **Apply** – Students organize, plan, record process, draft, record findings, and show the results of the performance lab or activity.
- **Reflect** – Students think about, and respond to, questions about the learning. Their responses focus on the content, product, process, and progress.



### B.4.3 Cooperative/collaborative work

Cooperative work occurs when students work in groups for extended periods of time. Students work together for the benefit of all group members. Research shows that cooperative learning environments stimulate cognitive activities in the areas of higher-order thinking, problem solving, and collaboration. Students who work in cooperative group situations reach objectives and goals with better accuracy than if they work individually on a task. Cooperative work is a foundation strategy used when instructors ask students to analyze and synthesize complex information. This strategy supports advanced thought processes, such as the creation of graphic organizers and the use of logical induction to solve problems. Students learn to be team players and acquire skills that will help them in their professions. Cooperative work occurs when students work in groups for extended periods of time to enhance the learning experience and create an energetic classroom atmosphere. Students might be grouped together as follows:

- Groups of two students to study online curriculum
- Groups of three students to complete cabling, lab, and programming activities
- Groups of five students to take oral exams and work as network or programming teams

There are a variety of ways to engage students through cooperative learning. Instructors can divide the class into student groups to conduct reviews, ask questions, learn content, and work on performance labs or other activities. It is important to know how and when to use groups for the most effective instruction. The following examples illustrate some of the types of groups and the purposes for which they might be used.

#### **Pairs or partners**

There are different methods that instructors can use to partner students:

- Each student can choose another student with whom they want to work.
- The instructor can assign partners.
- Students can work with other students based on the classroom seating arrangement.

Students can work in teams of two or they can form a larger group. Students can also partner with three students in classes with an odd number of students. A pair may partner with another pair so that the absence of one student will not disrupt their work.

#### **Small groups**

Small groups usually have three to five students. Small groups can be formed in the following ways:

- The students can choose their own partners.
- The instructors can assign members to a group.
- The students can work with other students based on the classroom seating arrangement.

The student roles within the group may be formal and assigned, or informal and unassigned. A formal or assigned role may be a leader, a speaker, a note taker, a summarizer, or a timekeeper. In informal groups, roles may be unassigned but naturally assumed by members of the group. Some group activities will not require the group members to assume any specific roles.

### **Teams**

A team usually has a specified purpose and consists of three to ten members. The team members may be assigned as follows:

- Appointed
- Selected by other members of the team
- Grouped informally based on classroom seating arrangements
- Selected alphabetically
- Selected through some other random method

Team members may or may not have assigned roles. This depends on the performance task. If there are specific roles, they may be based on skill, interest, or necessity. The end product or result of the team effort may contribute to the grades of all or individual team members.

### **Competitive teams**

The selection of team members for competitive team activities is similar to the previous description. Each competitive team has a specific purpose. They compete with other teams to determine which team can accomplish the criteria and objectives of a performance task with the most speed and accuracy. The members of each team receive rubrics and criteria for the task.

### **Large groups**

A large group of students can be configured in a variety of ways:

- Smaller teams
- Groups
- Partners
- Individuals
- Whole class

The parameters and criteria for large group discussion and participation should be established prior to the task or activity. This is done so that all of the team members understand their roles and responsibilities within the group.

### **Whole class**

This type of group is designed to involve all of the students. The parameters for participation and topic focus are clarified in advance so that all participants understand their roles and responsibilities within the class. This student configuration facilitates the following activities:

- Teacher-led discussions

- Student-led discussions
- Demonstrations
- Presentations

### **Web Links**

Teaching Strategies: Group Work and Cooperative Learning:  
<http://www.crlt.umich.edu/tstrategies/tsgwcl.html>

Enhancing Student Thinking through Collaborative Learning. ERIC Digest:  
<http://www.ericfacility.net/ericdigests/ed422586.html>

## B.4.4 Jigsaws

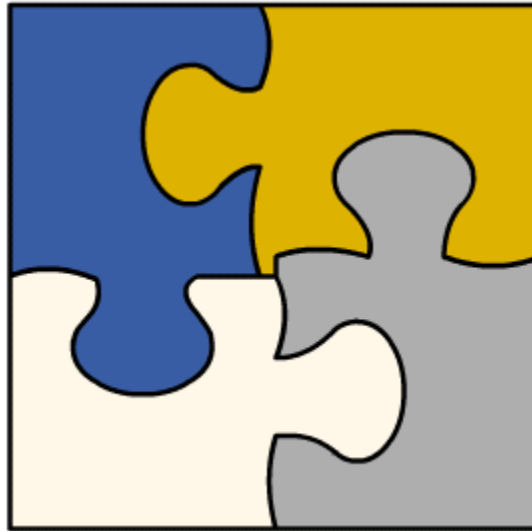


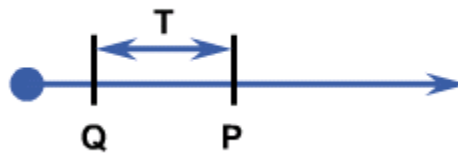
Figure 1: Jigsaw Puzzle

The teaching and learning strategy known as the expert jigsaw was configured by Elliot Aronson in the late 1970s. This strategy asks students to explore new information within the dynamics of a group setting. Cooperative group skills are a prerequisite for this type of learning. Students are divided into three groups, which are called home groups. Each group is assigned a number or a name. The content to be learned is broken into three sections. The content is distributed so each home group receives one of the three sections of content. The use of color codes is a useful technique to implement within this activity. Three different colors are used to distinguish between the three content sections to be learned. Members from each group move to an expert group where the main points of the content are discussed. Members of the expert group process this new information and return to their home groups to teach other members the main points of what they learned from the activity. Research states that this is one technique that stimulates significant learning within the brain since it requires critical analysis and articulation before the acquired knowledge can be taught to others.

### Web Links

Training: How To Do Tasks: <http://www.cvm.tamu.edu/wklemm/logic10.html>

## B.4.5 Ask the right questions



**Q = Question Asked**  
**P = Prompt Breaks Silence**  
**T = Wait Time**

**Figure 1: Ask the Right Questions**

In classrooms and labs across the United States, students are typically given questions that test their low-level and high-level cognitive abilities. Instructors who ask low-level questions expect students to respond with basic recall of facts and comprehension based on information they heard in a lecture or read from the curriculum. An example of a low-level question is to ask students to name the levels of the food pyramid or list the elements on the periodic table. This is the most common type of question that students are asked in schools. High-level questions are more open-ended and interpretive. Students are required to analyze and synthesize information. With high-level questions, students are asked to communicate their knowledge through logic, reasoning, and evidence. An example of a high-level question is to ask students to predict the next world epidemic or explain why rockets cannot launch into outer space in extremely cold weather.

The average wait time for teachers after they ask a question in a classroom is approximately 1.5 seconds. Research indicates that with just a 3-second waiting period, student answers are more accurate and organized. Instructors should ask students questions about the concepts that they will continue to understand long after the little details fade away from their short-term memories. These concepts will require teachers and students to reflect on the intrinsic value of the questions that they ask and the truths that these questions may uncover.

The late Dr. Mary Budd Rowe was an accomplished science educator at the University of Florida and Stanford University. Dr. Rowe studied classroom dynamics. One of Dr. Rowe's greatest contributions was to study the time between when an instructor finishes asking the class a question and when the instructor breaks the silence and prompts the class further to respond to the question.

Figure 1 shows a timeline. At time Q, the instructor finishes asking a question. At time P, the instructor breaks the silence, either with encouragement or the correct answer. Dr. Rowe called the time between Q and P the wait time. This concept can lead to significant improvements in student learning.

- The instructors who participated in the study had an average wait time of about 1 second after they asked a question and before they took further action to elicit a response. Dr. Rowe discovered that if the wait time was extended from about 1

second to beyond 3 seconds, the following significant improvements in classroom dynamics occurred:

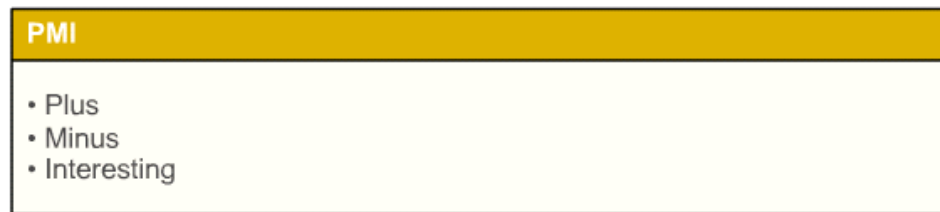
- Longer responses by students
- More participation by more students with more confidence
- Increase in student-to-student interactions
- More questions asked
- Improvements on complex assessments
- Better classroom management

Instructors who use question and answer techniques to teach networking should increase the wait time to see if student learning improves. Instructors can read an article written by Dr. Rowe to learn more about this concept.

Rowe, M., (1974). Relation of wait-time and rewards to the development language, logic and fate control: a. part one: wait time. Journal of Research in Science Teaching, 11(2), 81-94. b. part two: rewards. 11(4), 291-308.

Many resources about different forms of wait time are also available on the Web.

## B.4.6 PMI



**Figure 1: PMI**

Many of the best instructional strategies help students think about their thought processes, or engage in metacognition. Other strategies encourage students to use knowledge in new and innovative ways. There are many strategies that are currently implemented in classrooms. This section will discuss three methods that are linked to easily-understood instruction, which encourages higher student achievement.

The first method is called Plus, Minus, Interesting (PMI). This practice is metacognitive and asks students to evaluate their thoughts about new information. After students have read, heard, or interacted with new information, they create a T-chart. The left side of the chart includes an area for items that might qualify as plus, minus, or interesting. Students respond to the following questions in relation to specific content:

- What do they consider to be a Plus?
- What do they consider to be a Minus?
- What do they consider to be an interesting process, comment or question?

Students record their thoughts on the right side of the chart as they apply the categories to the new content. Students can work individually on PMI charts and then share their responses with a partner or a larger group. Ideas and perspectives are shared until they reach common conclusions. PMI is especially useful during lecture sessions since it provides students with an opportunity and a method to digest new content.

### Web Links

PMI: <http://www.mindtools.com/pmi.html>

Activating and Engaging Habits of Mind:

<http://www.ascd.org/cms/objectlib/ascdframeset/index.cfm?publication=http://www.ascd.org/publications/books/2000costa1/2000costatoc.html>

## B.4.7 Graphic organizers

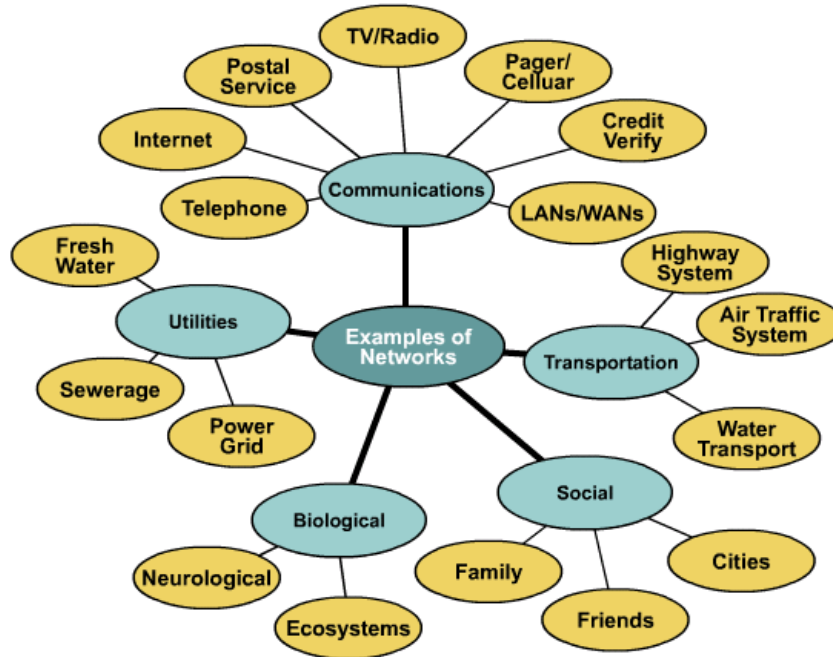


Figure 1: Cluster Diagram

Alternatives	Specifications				Totals
	Spec 1	Spec 2	Spec 3	Spec 4	
Idea A					<input type="text"/>
Idea B					<input type="text"/>
Idea C					<input type="text"/>
					<input type="text"/>

Figure 2: Problem-Solving Matrix



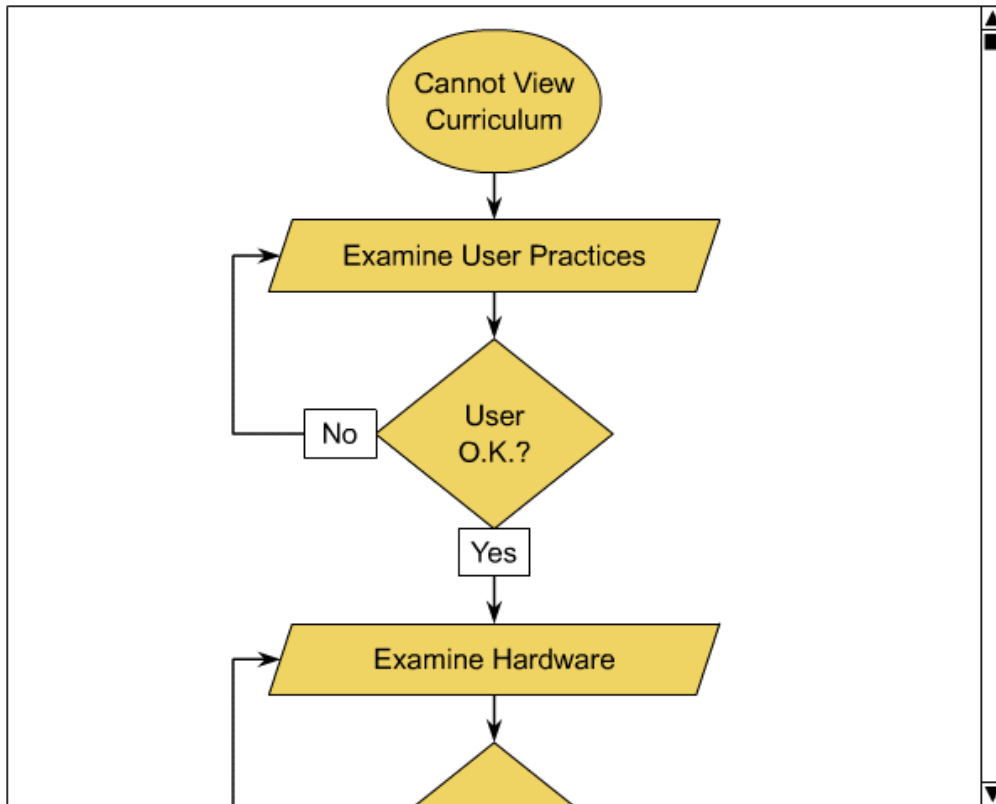


Figure 3: Flowchart

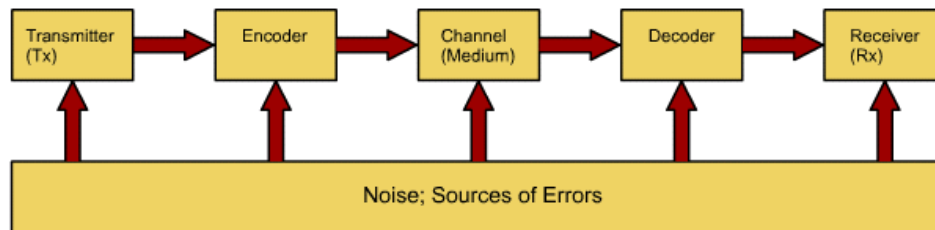


Figure 4: Block Diagrams

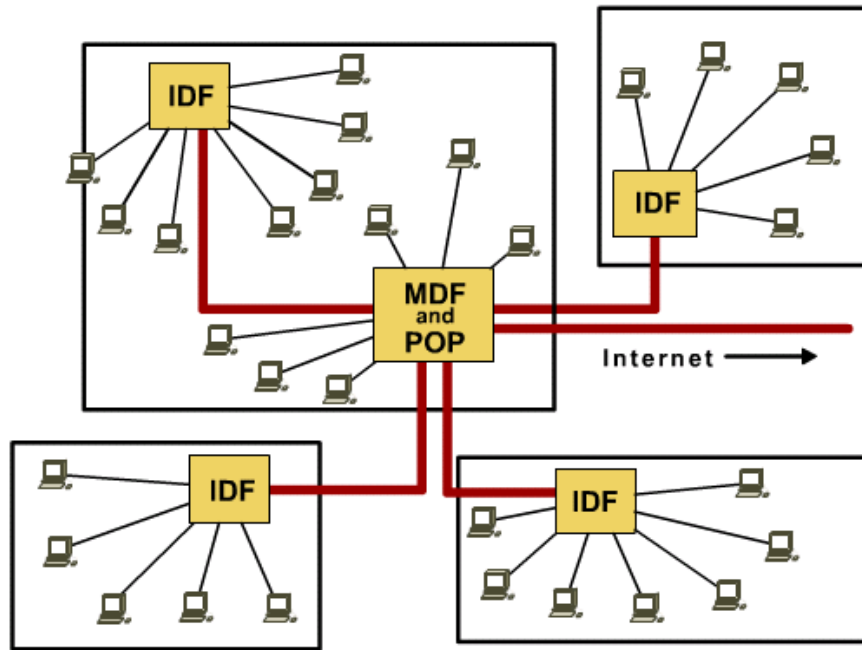


Figure 5: Extended Star Topology in a Multi-Building Campus

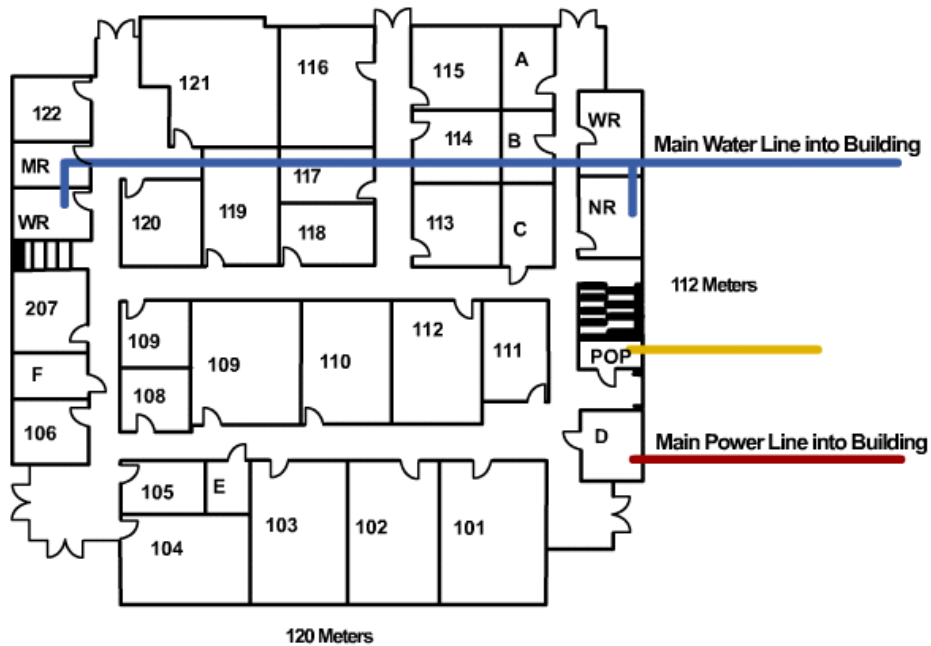


Figure 6: Main Building First Floor

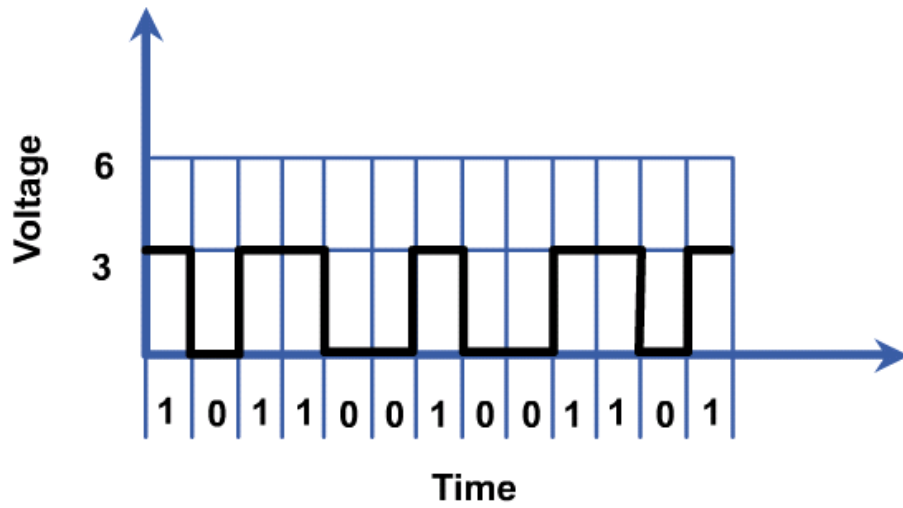


Figure 7: Digital Signal

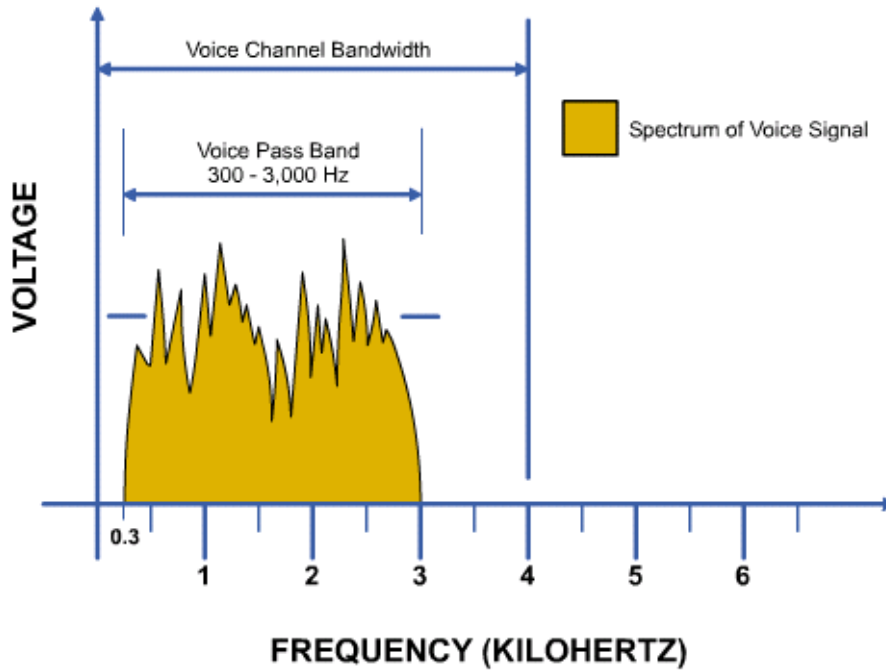


Figure 8: Spectrum Diagram of a Voltage versus Frequency Graph

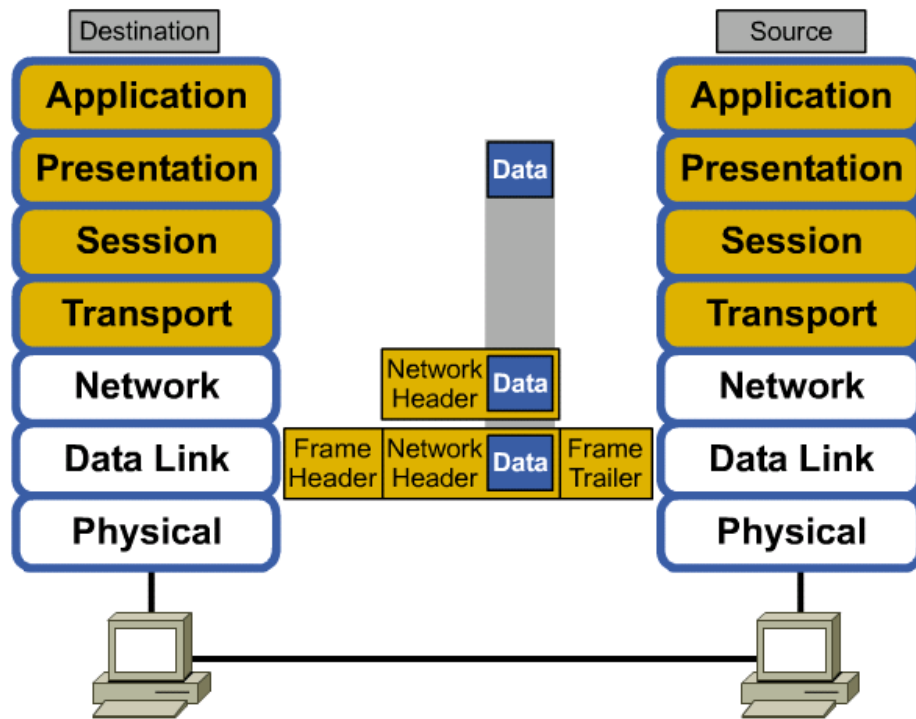
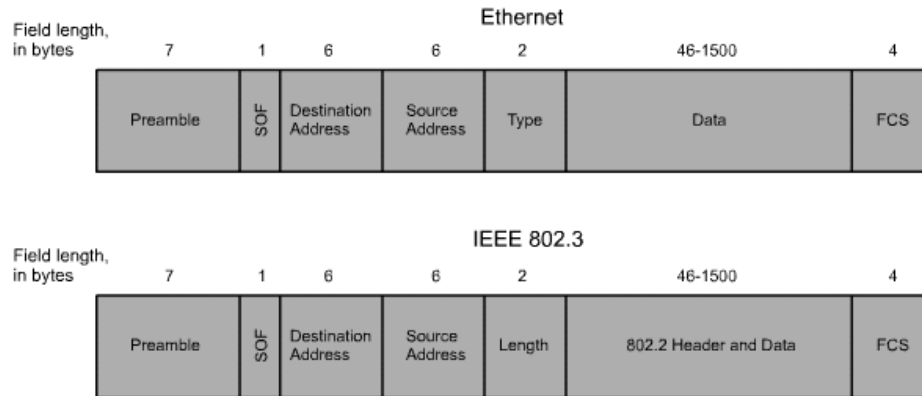


Figure 9: Data Encapsulation



SOF = Start-of-frame Delimiter  
 FCS = Frame Check Sequence

Figure 10: Ethernet and IEEE 802.3 Frame Format

### LANs are designed to:

- Operate within a limited geographic area.
- Allow multi-access to high-bandwidth media.
- Control the network privately under local administration.
- Provide full-time connectivity to local services.
- Connect physically adjacent devices.

### Using:

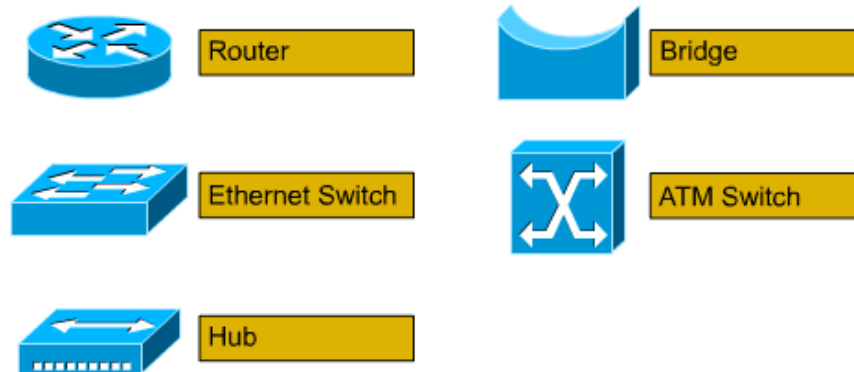


Figure 11: Local Area Networks and Devices

### WANs are designed to:

- Operate over large geographical area.
- Allow access over serial interfaces operating at lower speeds.
- Provide full-time and part-time connectivity.
- Connect devices separated over wide, even global areas.

### Using:

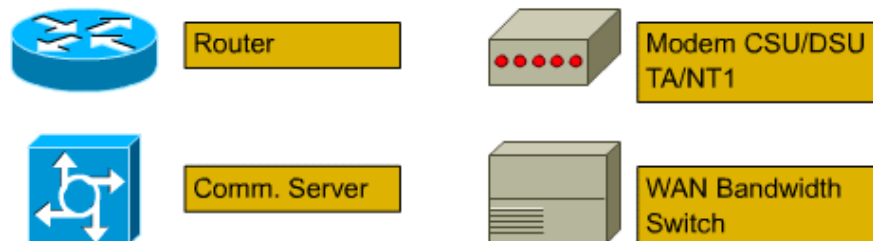


Figure 12: Wide Area Networks and Devices

Advanced organizers can be used to tap into the prior knowledge of students. There are many forms of advanced organizers such as exposition, narratives, and graphics. Graphic organizers are shown in Figures 1 through 12. These methods were publicized by a psychologist named David Ausubel in the late 1960s. These techniques help students make connections between their current knowledge and the information needed to reach a more complete comprehension of a learning objective. Graphic organizers also enable students to arrange large chunks of new information into smaller chunks. These smaller pieces are easier to learn and understand.

Cluster diagrams help students generate and organize thoughts. When students brainstorm, a question or concept is put in the center of a cluster and all of their ideas are added to the cluster. Similar ideas are grouped together. Cluster diagrams are also used as concept maps or to present course material to students. They can also be used to assess how well students understand a concept.

Problem-solving matrices are a standard part of design documentation. In their simplest form, a variety of design options such as network media, network architecture, or protocols are listed vertically and the specifications against which choices will be rated are listed horizontally. In theory, the option that earns the highest score against the specification rubric is chosen. However, design is a repetitious process and many layers of matrices are typically created with increasingly refined specifications, weighted rubrics, and significant brainstorming and research.

Flowcharts are a standard part of computer programming. Flowcharts and process flow diagrams are generally used to graphically represent various branches of a process. Flowcharts are used throughout the curriculum to describe configuration, troubleshooting, and communications processes.

Block diagrams are standard in the electronics industry. A few simple symbols or pictorials and arrows are used to indicate the flow of information. Block diagrams include simple descriptions of the functions of the various blocks. Block diagrams represent an intermediate level of detail for electrical systems. They are not circuit-level schematic diagrams. A block diagram of the following components is a good accompaniment to flowcharts that explain the processes that occur among the blocks:

- The internal components of a PC
- The internal components of a router
- The devices make up the LAN or a WAN

In networking there are logical topological diagrams and physical topological diagrams. Logical topologies refer to logical interconnections and the flow of information in a network. Physical topologies refer to the devices, ports, interconnections, and physical layout of a network. Both of these diagrams are used extensively.

Electrical engineers refer to voltage versus time graphs of signals as the time domain. These graphs show the output from an oscilloscope, which is a device that measures voltage. These graphs summarize many important networking concepts, particularly in the first semester curriculum:

- Bits
- Bytes
- Analog signals
- Digital signals
- Noise, attenuation
- Reflection

- Collision
- AC
- DC
- RFI
- EMI
- Encoding
- Transmission errors

### **Web Links**

David Ausubel: Advance Organizers

<http://chd.gse.gmu.edu/immersion/knowledgebase/strategies/cognitivism/AdvancedOrganizers.htm>

## B.4.8 Setting goals

Students perform well when they have a plan and access to the necessary resources. The research on goal setting and its impact on learning is impressive. There are certain truths for students who set personal achievement goals.

When students set personal achievement goals, they can identify and connect to a greater purpose to reach their goals. Students identify how a goal fits into their future plans through reflection, problem solving, and decision-making. Students define the steps they need to take to reach long-term and short-term goals. They set criteria for each level of achievement and conjure up a mental picture of the results they want. Personal goals give students a map for their success. It is important to create a design or an intended course of action. Students should list the small steps and the larger milestones and use visual reminders. Students demonstrate their dedication to reach their final goals through progress. The achievement of a goal is only possible if students are willing to make decisions and modify their behavior along the way. Students must dedicate their strengths and resources to the goal in spite of any diversions, disappointments, or difficulties they encounter.

To successfully reach their goals, students need to make connections with other people. They should seek out people with the knowledge to advance their comprehension and the passion to keep them motivated and encouraged. It is a fundamental psychological principal that learning requires the assimilation of new comprehension into a current level of comprehension. Students can be shown how to tap into their personal experiences and knowledge to find solutions to their problems.

Finally, there must be an evaluation process. Students should measure their accomplishments at each level of their action plan. Students will continuously put additional procedures in place to help them reach the next step toward their goals. Instructors who advocate the practice of goal-setting in their courses should provide opportunities to discuss goal-setting skills as they pertain to personal goals. These instructors can demonstrate time-management skills in the classroom and monitor student goal-setting behaviors. Instructors should set aside time for students to determine their progress. This can be done through reflection and journal writing activities. Instructors also demonstrate risk-taking behaviors in the classroom. They encourage their students to try new strategies if they believe a strategy may help them reach their goals.



## B.4.9 Kinesthetic activities

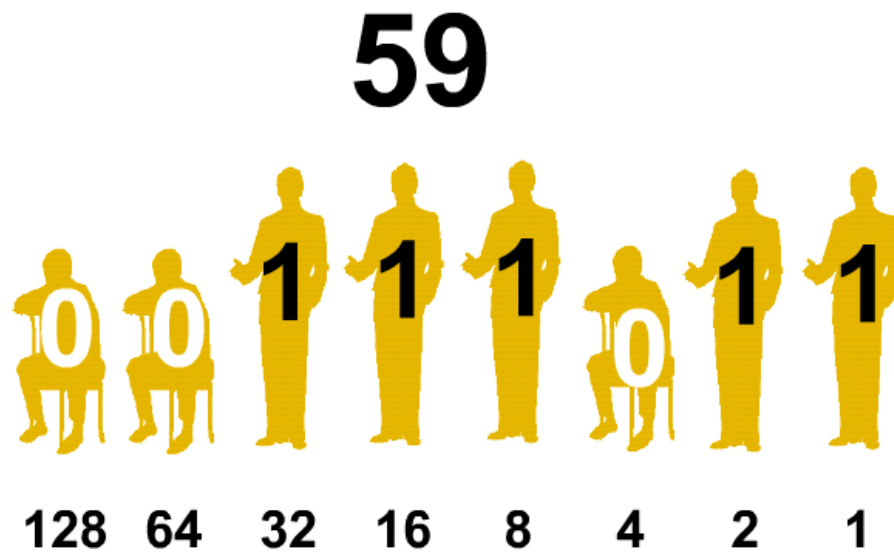


Figure 1: Kinesthetic Activities

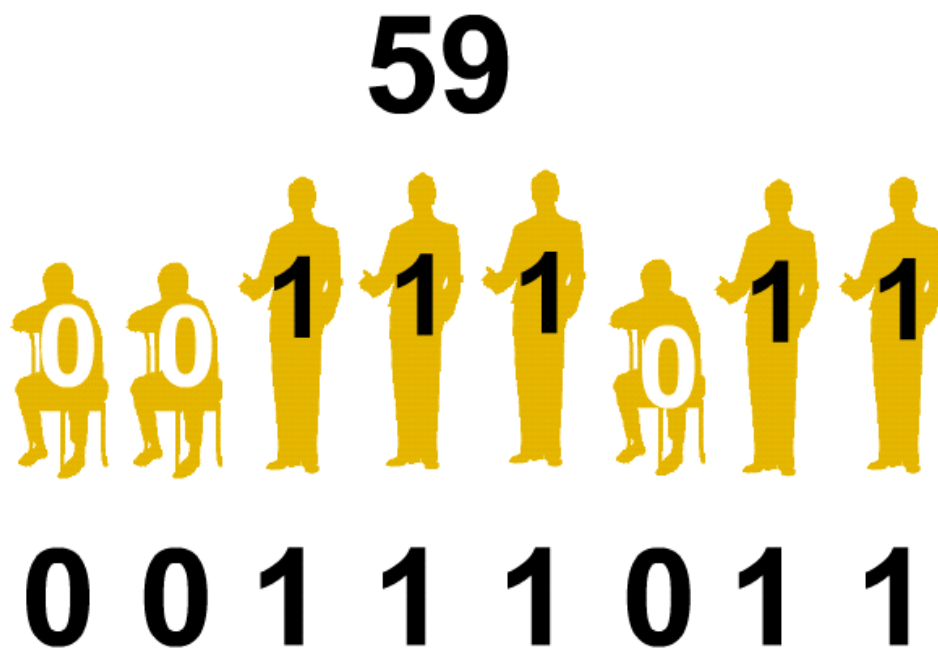


Figure 2: Kinesthetic Activities

A kinesthetic activity refers to the movement of the body to act out or communicate something. The kinesthetic activities in this section demonstrate the networking process. These exercises are also known as role-playing activities or skits. They help students understand complex and normally invisible processes. Kinesthetic activities can be a helpful way to introduce basic IT concepts. Most IT courses require knowledge of binary arithmetic. Figures 1 and 2 show an activity that can be done with eight students. Each student represents a specific place value of 128, 64, 32, 16, 8, 4, 2, or 1 for 8-bit binary numbers. The instructor picks a number between decimal 0 and 255 and each student must decide if they should sit to represent binary 0 or stand to represent binary 1. Many IT processes and algorithms can be expressed through kinesthetic activities.

Role-playing occurs when students act out or dramatize a scenario, story, event, or real life situation. Role-playing activities can be used to help students understand events, discoveries, or interpersonal relationships. Students can create a script for role-playing or ad-lib the actions and dialogue.

### **Web Links**

Kinesthetic Teaching: <http://www.mindsinmotion.org/creative.html>

## B.5 Assessment Strategies

### B.5.1 Review strategies

Most lessons contain review questions that pertain to content from the previous lesson. Strategies for the use of review questions can be selected from the following list:

- Individual students answer review questions on their computers.
- Pairs of students discuss and answer review questions on their computers.
- Pairs or small groups of students discuss and answer review questions before each student completes the review.
- The entire class or groups of students discuss review questions and enhance their levels of comprehension through the discussion.
- Small groups each discuss a portion of the questions and explain their findings to other groups to demonstrate their knowledge. This is an example of the jigsaw technique.
- The entire class plays a game in which one person states a fact, which represents the correct answer to a question, and leaves out an important piece of information. The rest of the class must respond with the missing information in the form of a question. For example, the fact could be “This is the first layer of the OSI” and the correct response would be “What is the physical layer?” Points can be awarded for correct responses based on the level of difficulty.
- Student teams or small groups design analogies to explain concepts to other teams of students.

### Web Links

Learning Through Technology: <http://www.wcer.wisc.edu/nise/cl1/ilt/default.asp>

## B.5.2 Journals and reflection

An effective evaluation practice for students is to write in journals and reflect on academic experiences. Students can document their individual learning process and highlight important concepts. A learning log asks students to document their learning steps and indicate what is clear, what confuses them, and what they would like to learn more about. This provides important information about how students interact with, and process, new content. Instructors can determine if students are satisfied with their program and motivated to continue. Journals are self-reflective and encourage students to reveal personal thoughts, feelings, and ideas. Some students may choose not to share this type of information. If instructors decide to practice this type of assessment in their classrooms, there must be clear communication between the instructor and the students about the purpose of this activity.

The teaching and learning environment is strengthened when instructors and students take time each day for reflection. Metacognition occurs when people think about their thought processes. This can be done through written, verbal, kinesthetic, or musical activities. Reflection is an important tool to develop new comprehensions about the world. When students ask essential questions about their learning experiences, they can improve their information processing skills and become better problem solvers and communicators.

Journals provide a space for inner thought and reflection on experiences that occur in the teaching and learning process. Instructors that incorporate journal writing into curriculum will usually set aside a period of time for this process. The teacher and students can use this time to reflect on completed tasks or make predictions about future experiences. Thoughts and ideas can be written down in a dedicated, personal paper space or in a word processor file. These thoughts can take many forms such as words, sentences, illustrations, maps, charts, magazine pictures, and newspapers. Journal entries can take the form of guided or free-style writing. Through this type of reflection, teachers and students can track their comprehension of issues and themes over time.

Academy instructors may want to instruct students to keep a technical or engineering journal to record details about all aspects of their network design and installation experiences. This may not seem important at first. However, it will help students develop a habit that will become more important as they increase their networking experiences. These journals are usually paperbound composition books in which pages are dated and added, but never removed. The entries would include things such as daily reflections, troubleshooting, details, procedures and observations, equipment logs, hardware and software notes, and router configurations.

Student reflection is an important element of instruction with limited time requirements. The process helps students analyze and become more responsible for their learning. During reflection, the students think about an aspect of the lesson and write a reaction in the study guide. This internalization of learning helps the students set goals and make sense of the learning process. It also links prior learning to present and future learning. The reflection process helps students analyze and synthesize new comprehension. Students use the cognitive processes of assimilation and accommodation to move learning from short term to long-term memory. After each lesson, students should reflect on one or more of the following categories:

- Content
- Product
- Process

- Progress

Throughout the year, students should review their reflections and acknowledge the growth in their comprehension. Prior to a reporting period, students should write a brief paper that explains their growth in knowledge and the skills they acquired in the preceding weeks.

Some examples of reflection and journal writing for Academy courses are as follows:

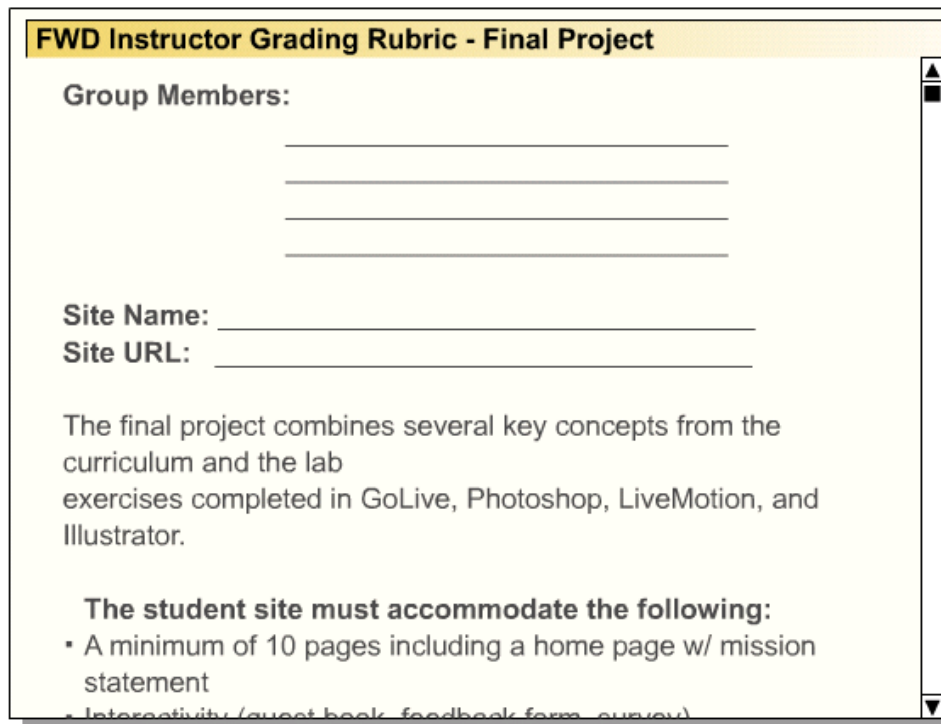
- Key ideas from class presentations
- Discussions
- Activities related to lesson content
- Personal analysis that shows a connection with the content purpose
- Questions or statements that indicate a need for further clarification or inquiry
- Attention to the process required to accomplish an important task
- Application of learned material to other content or subjects
- A demonstration of the connection between concept or content
- Thoughtfulness as demonstrated by goals for improvement
- Other actions that demonstrate self-learning
- Acquired knowledge
- Important concepts
- Skills
- Improvements
- Effective strategies
- Ineffective strategies
- Group activities
- Instructor performance
- Progress
- Shortcomings
- Goals for further learning
- Applications of knowledge

## Web Links

Student Reflection Questions:

<http://pblmm.k12.ca.us/PBLGuide/PlanAssess/StReflectionQuestions.html>

## B.5.3 Rubrics



**FWD Instructor Grading Rubric - Final Project**

**Group Members:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Site Name:** \_\_\_\_\_

**Site URL:** \_\_\_\_\_

The final project combines several key concepts from the curriculum and the lab exercises completed in GoLive, Photoshop, LiveMotion, and Illustrator.

**The student site must accommodate the following:**

- A minimum of 10 pages including a home page w/ mission statement
- Interactivity (guest book, feedback form, survey)

**Figure 1: Grading Rubric Sample**

Another good instructional practice is the use of rubrics as a form of assessment. A rubric allows criteria to be established for outcomes that are acquired through individual or group projects. Levels of success and quality are identified at different levels of a predetermined scale. Quantitative data can be associated with each level of performance. Rubrics assess observable learning behavior, all curriculum content associated with a project, and other components such as design, research skills, organization of thought, cooperative skills, and the ability to communicate emerging knowledge. The rubric has two primary functions for teaching and learning. Rubrics communicate expectations and give students a level of achievement to work toward. One of the most important benefits of rubric assessment is the control it gives to students. Students can create their own rubrics based on established standards and performance objectives. Assessment occurs continuously through self-monitoring and self-evaluation. Students who are given direction and the freedom to choose their path of learning, are empowered to accomplish high levels of achievement.

For Academy courses, rubrics create specific expectation criteria for the final performance of a lab or activity. In the demonstration of each task, there is a specific set of performance levels for all objectives, content, and skills. Each rubric contains a criterion that defines the elements that indicate learning proficiency. Many rubrics are based on a four-point scale, where four points represent the best level. Each point on the scale has specific criteria that describe the performance characteristics. Before an assessment of student interactions, classroom work, or any performance lab or activity, students should be aware of the expectations. This will help them begin the process of self-assessment as they progress through the individual tasks that are reflected in the rubric.

Rubrics that are developed by both students and teachers can help students organize and prepare for learning through advance knowledge of their assessment expectations. It also allows students to contribute to the development of the grading scale for their performance labs or activities.

### **Web Links**

RUBISTAR: <http://rubistar.4teachers.org/>

Rubrics and Assessments: <http://home.socal.rr.com/exworthy/rubric.htm>



## B.5.4 Portfolio

A portfolio is an example of authentic assessment. As students complete major presentations or networking projects, they save them in a portfolio. A portfolio of accomplishments must be presented before many companies will hire an individual. Portfolios show growth over time and include student reflections on different periods of learning. Academy students might keep a portfolio of their experience in building a network and examples of configurations they created for different scenarios. Community projects are also good examples of accomplishments.

A portfolio is a paper, electronic, or online collection that shows the best work of a student. As with any educational initiative, portfolios are continually revised and improved. Many secondary school districts encourage portfolio-based assessments. The Cisco Networking Academy Program is well suited for this type of assessment. Students maintain their portfolios to include all of their best work throughout all semesters of a curriculum. This portfolio can contribute to graduation criteria. It can also serve as an impressive display for potential employers.

### Web Links

Guidelines for Portfolio Assessment in Teaching English:  
<http://www.etni.org.il/ministry/portfolio/default.html>

## B.5.5 Oral exams

Date/Time/Place:						
Group#	Time (25 min slots)	Member #1	Member #1	Member #1	Member #1	Member #1
1	3:00-3:25					
2	3:30-3:55					
3	4:00-4:25					
4	4:30-4:55					
5	5:00-5:25					
6	5:30-5:55					

**NOTE: ANY MEMBER OF ANY GROUP MAY BE ASKED ANY OF THESE QUESTIONS!**

**Learning Goals**

- Encouraging students' skills in quick recall of facts and concepts and "thinking on their feet."
- Assessing student understanding in ways deeper than multiple-choice questions.
- Learning professional standards for answering questions and articulating concepts orally under time pressure.
- Engaging students' multiple intelligences and providing a prompt for group-based surviving and learning.

Figure 1: Oral Exams

#	Time Limit (minutes)	Prompt (exact wording given to student)	Point Value	Sample Responses (to earn that point value)
1	5	<p>Give the student a situation (a school to be wired or a project they completed during the semester)</p> <p>Choose media, justifying your choice with a matrix</p> <p>Draw a simple physical topology, locationing POP, MDF, IDF, MCC, ICC, HCC backbone. Justify all choices of locations.</p> <p>Draw a simple flowchart of what you would do to design, install, and test the cabling you've intalled</p>	4	<p>+1 for comparison of media choices and proper use of matrix</p> <p>+2 for reasonable locations and justifications</p> <p>+1 for a chart which include planning porcesses, installing jacks, stringing cable, and using test equipment</p>

Figure 2: Oral Exams

Well-planned oral examinations can be powerful learning experiences for students. Careful preparation can minimize the intimidation that is felt by some students. The models for oral exams are usually based on job interviews and graduate school oral exams. A method that works particularly well for groups of diverse students, is to give teams of students the exam questions, answers, and rubrics prior to the exam session. Establish scheduled exam times, which can be after school if necessary. Students study and complete assessment activities in groups. Then, each individual member of a team enters the room alone and is asked one of the questions by the board. The students do not know which question they will be asked in advance. This method of oral testing usually motivates the students to study hard and with a lot of enthusiasm. Examples of oral exams are found in Semester 2 Lesson Plans. Instructors are encouraged to develop their own techniques for oral examinations and should use them to test for benchmark comprehension.

## B.5.6 Lab exams

**Lab Exam/Skills Exam Examples from Academy Curriculum**

Curriculum	Vendor	Skills Tested
CCNA	Cisco	
CCNP	Cisco	
IT Essentials	HP	
Fundamentals of Voice and Data Cabling	Panduit	
Unix	Sun	
Java	Sun	
Web Design	Adobe	

**Figure 1: Lab Exams**

Lab exams are also known as skills exams. These exams give students an opportunity to demonstrate their knowledge of cable and router configuration. Students use cables and routers to assemble a network in a lab. Their performance task is to connect cables and routers so every router can successfully communicate with the other routers. The number of routers to connect will vary based on equipment access. This process is one that distinguishes the Cisco Networking Academy Program from all other programs. When students graduate from the Academy, they have been tested on their hands-on expertise with equipment. This practice supports authentic assessment and gives students higher credibility in the job market.

Lab exams include all of the following:

- Practical exams
- Performance exams
- Demonstration labs
- Skills-based and performance assessments
- Authentic assessment
- Mastery learning
- Formative and summative exams

Cisco recommends a simple pass or fail grade, with opportunities to retake the skills exam if necessary.

## Web Links

Certification Magazine: [http://www.certmag.com/issues/aug01/feature\\_long.cfm](http://www.certmag.com/issues/aug01/feature_long.cfm)

CCIE: <http://www.cisco.com/warp/public/625/ccie/>

## B.5.7 Six lenses

Six Lenses
<ul style="list-style-type: none"><li>▪ Equity</li><li>▪ Curriculum</li><li>▪ Teaching</li><li>▪ Learning</li><li>▪ Assessment</li><li>▪ Technology</li></ul>

Figure 1: Six Lenses

In any learning endeavor, certain lenses are indispensable to ensure a high quality experience for students. There are six different perspectives that are supported in the Academy courses:

- Equity
- Curriculum
- Teaching
- Learning
- Assessment
- Technology

It is important to ask questions about these factors in all Academy curriculums. The following example uses UNIX:

- **Equity** – Do all Academy students have adequate access to information about UNIX?
- **Curriculum** – Do the online curriculum and skills-based labs provide ample opportunities for students to learn about UNIX?
- **Teaching** – Do all Academy students have access to instructors who use instructional best practices to teach UNIX?
- **Learning** – Do students have adequate resources to construct their own iterative comprehension of UNIX?
- **Assessment** – Do all students have access to online and skills-based formative and summative assessments?
- **Technology** – What technologies enable the effective teaching of UNIX?

As instructors work through this orientation they are encouraged to revisit these essential questions. In this section, Cisco presented some useful content, tools, and perspectives. Ultimately, instructors should decide what teaching methods are best for their students.