ICND1

Interconnecting Cisco Networking Devices Part 1

Course Administration Guide

For Student Guide

Version 1.0

Text Part Number: N/A

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

ICND1

Course Management

Cisco CCNA Curriculum Changes in 2007

Designed to Job Tasks

The CCNA® curriculum was revised in 2007 to teach and test job tasks, skills, and knowledge that are expected of a CCNA graduate. Course and exam objectives were designed from the job tasks:

- Describe how a network works
  - Describe the purpose and functions of various network devices
  - Select the components required to meet a network specification
  - Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
  - Describe common networked applications, including web applications
  - Describe the purpose and basic operation of the protocols in the OSI and TCP models
  - Describe the implementation of VoIP in a small network
  - Interpret network diagrams
  - Determine the path between two hosts across the Internet
  - Describe the components required for network and Internet communications
  - Identify and correct common network problems at Layers 1, 2, 3, and 7 using a layered model approach
  - Differentiate between LAN and WAN operation and features
- Configure, verify, and troubleshoot a switch with VLANs and interswitch communications
  - Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
  - Explain the technology and media access control method for Ethernet networks
  - Explain network segmentation and basic traffic management concepts
  - Explain basic switching concepts and the operation of Cisco switches

- Perform and verify initial switch configuration tasks, including remote access management
- Verify network status and switch operation using basic utilities (ping, traceroute, telnet, SSH, ARP, ipconfig), **show** and **debug** commands
- Identify and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures
- Describe enhanced switching technologies (VTP, RSTP, VLAN, PVST, 802.1Q)
- Describe how VLANs create logically separate networks and the need for routing between them
- Configure, verify, and troubleshoot VLANs
- Configure, verify, and troubleshoot trunking on Cisco switches
- Configure, verify, and troubleshoot inter-VLAN routing
- Configure, verify, and troubleshoot VTP
- Configure, verify, and troubleshoot RSTP operation
- Interpret the output of various **show** and **debug** commands to verify the operational status of a Cisco switched network
- Implement basic switch security (port security, unassigned ports, trunk access, management VLAN other than VLAN1, and so on)

- Implement an IP addressing scheme and IP services to meet network requirements
  - Describe the operation and benefits of using private and public IP addressing
  - Explain the operation and benefits of using DHCP and DNS
  - Configure, verify, and troubleshoot DHCP operation on a router
  - Implement static and dynamic addressing services for hosts in a LAN environment
  - Configure a device to support NAT and DHCP
  - Calculate and apply a VLSM IP addressing design to a network
  - Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN or WAN environment
  - Describe the technological requirements for running IPv6 (that is, protocols, dual stack, tunneling, and so on)
  - Describe IPv6 addresses
  - Identify and correct common problems associated with IP addressing and host configurations
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices
  - Describe basic routing concepts (packet forwarding, router lookup process)
  - Describe the operation of Cisco routers (router bootup process, POST, router components)
  - Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
  - Configure, verify, and troubleshoot RIPv2
  - Access and use the router CLI to set basic parameters

  - Connect, configure, and verify operation status of a device interface
  - Verify device configuration and network connectivity using ping, traceroute, Telnet, SSH, or other utilities
  - Perform and verify routing configuration tasks for a static or default route given specific routing requirements
  - Manage Cisco IOS configuration files (save, edit, upgrade, restore)
  - Manage Cisco IOS Software
  - Compare and contrast methods of routing and routing protocols
  - Configure, verify, and troubleshoot OSPF
  - Configure, verify, and troubleshoot EIGRP
  - Verify configuration and connectivity using ping, traceroute, and Telnet or SSH
  - Troubleshoot routing implementation issues
  - Verify router hardware and software operation using **show** and **debug** commands
  - Implement basic router security

- Install a small wireless network
  - Describe standards associated with wireless media (802.11a/b/g/n, Wi-Fi)
  - Identify and describe the purpose of the components in a small wireless network
  - Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
  - Describe wireless security concerns and explain how to configure WPA security (open, WEP, WPA1, and WPA2)
  - Identify common issues with implementing wireless networks
- Identify security threats to a small network and describe general methods to mitigate those threats
  - Describe today’s increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats
  - Explain general methods to mitigate common security threats to network devices, hosts, and applications
  - Describe the functions of common security appliances and applications
  - Describe security recommended practices including initial steps to secure network devices
  - Describe the components of a VPN (importance, benefits, role, impact)
  - Identify VPN client issues
  - Implement and troubleshoot NAT and ACLs
  - Describe the purpose and types of ACLs
  - Configure and apply ACLs based on network filtering requirements
  - Configure and apply an ACL to limit Telnet and SSH access to the router
  - Verify and monitor ACLs in a network environment
  - Troubleshoot ACL implementation issues

  - Explain the basic operation of NAT
  - Configure NAT for given network requirements using the CLI
  - Troubleshoot NAT implementation issues
- Implement and verify WAN links
  - Describe different methods for connecting to a WAN
  - Configure and verify a basic WAN serial connection
  - Configure and verify Frame Relay on Cisco routers
  - Configure and verify a PPP connection between Cisco routers
  - Troubleshoot WAN implementation issues

CCNA Curriculum in the Certification Pyramid

Changes to the CCNA curriculum are intended to maintain the integrity and quality of the CCNA certification as the premier industry networking certification. CCNA remains the foundation for Professional and Expert certifications, and for many Specialist certifications.

The CCNA curriculum was adjusted in mid-2007 to better fit and prepare for the Cisco CCNP® curriculum, as revised earlier in 2007. Topics and skills are introduced in CCNA as preparation for further study in the CCNP curriculum. The Course Administration Guides specify the depth to teach on these topics, and when to recommend more advanced courses to learners.

A new Cisco Certified Entry Networking Technician (CCENT) certification was introduced in mid-2007. The CCENT certification is attained by passing the ICND1 exam. This produces a new certification—less than CCNA, but a preparation for and partial completion of CCNA. CCENT certification may also be used as a prerequisite for specializations that do not require all of the skills and knowledge of CCNA.

During the transition from INTRO/ICND to ICND1/ICND2, the CCNA Certification website details how to quality for CCNA certification by passing combinations of INTRO/ICND/CCNA and ICND1/ICND2/CCNA exams.

ICND1 and ICND2 Compared to INTRO and ICND

Designed to Job Tasks

The CCNA curriculum was revised to base all topics and activities on job tasks expected of a CCNA graduate. Course objectives were revised to teach and practice these job tasks. The list of job tasks for the curriculum were subdivided into task lists for each course. Each task list includes all skills and knowledge taught in the course, and the Course Administration Guide specifies the depth to teach for each task. The course task list is detailed in the Course Administration Guide for the course.

Two Equally Balanced Parts

The CCNA curriculum is now composed of two balanced courses. Each course is a self-contained course with labs positioned throughout to practice skills soon after discussion. Each is a five-day course.

ICND1 Goal

Upon completing the ICND1 course, the learner should have the knowledge and skills necessary to install, operate, and troubleshoot a small branch office enterprise network, including configuring a switch, a router, connecting to a WAN, and implementing network security. A learner should be able to complete configuration and implementation of a small branch office network under supervision.

ICND2 Goal

Upon completing the ICND2 course, the learner should have the knowledge and skills necessary to install, operate, and troubleshoot a small to medium-size branch office enterprise network, including configuring several switches and routers, connecting to a WAN, and implementing network security. A learner should be ready to participate on an implementation team to implement a small- to medium-size branch office network, and to serve on a tier-one help desk or Network Operating Center.

Lessons have been moved from ICND (ICND2) forward into ICND1. PPP, NAT/PAT, and RIP2 are introduced and configuring skills are developed in ICND1. In ICND2, more advanced skills build on these foundations. This shift of topics results in a more comfortable time budget for ICND2.

ICND1 is a prerequisite to ICND2; a learner cannot participate in and complete ICND2 without mastering the skills and knowledge in ICND1. Unlike INTRO, ICND1 is not simply a collection of background topics, but is a complete, self-contained course with frequent lab practices.

Topics Added and Deleted

ISDN and Interior Gateway Routing Protocol (IGRP) topics have been removed as outdated and are no longer commonly encountered at an Associate level.

New Topics and Lessons Added

Network security topics and lessons have been added. Learners secure switches, routers, ports, and implement basic network security. Learners do not design security policy, but only implement basic security measures according to a given policy.

Connecting a wireless LAN (WLAN) to a network was added to ICND1. Only the client security aspects are discussed. The learner is not expected to implement wireless access points. The learner troubleshoots client connectivity. To avoid the expense of adding WLAN equipment, no lab is specified

Learners are still directed to verify changes and configurations they have made. Troubleshooting topics and lessons have been added to broaden the job tasks of a CCNA graduate. Troubleshooting tasks are positioned as part of day-to-day or “day two” activities. A CCNA would be expected to perform elementary troubleshooting when acting as members of a Network Operations Center or Help Desk.

Although Telnet is still taught, learners are encouraged to employ SSH as the preferred method of remotely accessing devices.

Learners are expected to be proficient configuring both CLI and Cisco Router and Security Device Manager (SDM).

Labs

ICND1 and ICND2 are each five-day courses to provide more learner practice in labs. Lab activities are about 40 percent of each course time budget. This ratio of lecture to lab can be further refined.

Labs occur throughout the courses, requiring learners to practice each set of skills and job tasks soon after they are discussed. Labs are positioned within modules, but can be collected at the end of each module at the convenience of the instructor's lesson plan, or availability of lab equipment.

All labs are designed for remote access.

The Lab Topology and Equipment List are common to both ICND1 and ICND2. Currently available Cisco equipment is specified, including Cisco integrated services routers (ISRs). Note that the specified Cisco IOS Software version introduces a restriction on device naming; this is documented in the Course Administration Guides and Lab Guides.

Labs are not "cookbook" labs; learners are not expected to rigidly type each step in the Lab Guide. The Course Administration Guide describes how to introduce and conduct each lab. The Student's Lab Guide presents the objective and scenario for the lab and a series of tasks to be performed. A solution or sample is provided at the end of the Lab Guide. The instructor should reference the Course Administration Guide and employ the Lab Guide to mentor learners during labs, maximizing their hands-on experience.

The concluding lab activity of ICND1 is a "capstone" lab, in which the learner will pull together all the knowledge and skills of the course to implement a small branch office.

The first module, and the first learner activity, of ICND2 is a "warm-up" lab. Learners review and practice the skills and knowledge of the prerequisite ICND1 to implement a small branch office network. This network is the basis for ICND2 labs, in which the learner extends the features and functionality of the network. This lab is positioned at the beginning of the ICND2 course to allow the instructor to access learner completion of the prerequisites and assess their readiness to deepen their skills and knowledge in ICND2.

ICND1 Course Management

Overview

What does a network administrator need to know to support their network? The answer to this question depends on the size and complexity of their network. Fortunately, regardless of size and complexity of the network, the starting point for *learning* to support a network is the same. This course is intended to be that starting point.

This course focuses on providing the skills and knowledge necessary to implement and support a small switched and routed network. For the purpose of this course, a small network is defined as 1 to 20 hosts connected to a single switch, with the switch running a single VLAN (VLAN1). The switch is also connected to a router providing a routed link (Routing Information Protocol [RIP] and default) to a simulated Internet and corporate office.

This course works from the bottom up, providing knowledge and skills as they are needed. The course starts with an introduction to networks. It then introduces host-to-host communications using TCP/IP. Next, Layer 2 devices (switches) are introduced into the network. Next, Layer 3 devices (routers) are introduced into the network. The introduction of Layer 3 devices leads to the use of WANs and routing to connect the site to the Internet and corporate sites. Finally, device management skills (Cisco Discovery Protocol, TFTP, and so on) are introduced.

As each set of knowledge and skills is introduced, a set of labs is provided to allow the learner to reinforce these skills. A capstone lab is provided as a final learning exercise. This lab presents the learners with a preconfigured network that matches the topology that they have used in the previous labs. A series of configuration errors are introduced in the lab configuration. The goal for the learners is to identify and correct these issues.

Outline

The Course Management section of the Course Administration Guide includes these topics:

- Overview
- Course Instruction Details
- Course Evaluations

The Lab Setup section of the Course Administration Guide includes these topics:

- Hardware and Software Requirements
- Delta Information for *Interconnecting Cisco Networking Devices Part 1* v1.0

Course Version

This course is the original release of the course named *Interconnecting Cisco Networking Devices Part 1* (ICND1) v1.0.

This course supersedes *Introduction to Cisco Networking Technologies* (INTRO) v2.1.

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe how networks function, identifying major components, function of network components, and the OSI reference model
- Using the host-to-host packet delivery process, describe issues related to increasing traffic on an Ethernet LAN and identify switched LAN technology solutions to Ethernet networking issues
- Describe the reasons for extending the reach of a LAN and the methods that can be used, with a focus on RF wireless access
- Describe the reasons for connecting networks with routers and how routed networks transmit data through networks using TCP/IP
- Describe the function of WANs, the major devices of WANs, and configure PPP encapsulation, static and dynamic routing, PAT, and RIP routing
- Use the command-line interface to discover neighbors on the network and manage the router startup and configuration

Target Audience

The primary audience for this course is as follows:

- Network administrators
- Network engineers
- Network managers
- Systems engineers

The secondary audience for this course is as follows:

- Network designers
- Project managers

Learner Skills and Knowledge

The knowledge and skills that a learner must have before attending this course are as follows:

- Basic computer literacy
- Basic Microsoft Windows navigation skills
- Basic Internet usage skills
- Basic e-mail usage skills

Course Instruction Details

This topic provides the information that you need to prepare the course materials and set up the classroom environment.

Instructor Requirements

To teach this course, instructors must have attended the following training or completed the following requirements:

- Active Certified Cisco Systems Instructors who have been certified to teach INTRO and ICND must complete the CCNA Instructor Update Briefing.
- All other Certified Cisco Systems Instructors in good standing will need to do the following:
  - Complete the ICND1 course as a learner.
  - Attend the ICND2 course as a learner.
  - Pass the CCNA certification test (or both the ICND1 and ICND2 certification tests).
  - If the certification test has yet to be taken but the courses have been completed, certifications will be provisional. The guidelines for ICND v2.2 instructors apply.
- A Certified Cisco Systems Instructor who is certified in technology and a WAN-certified instructor are part of a “common pool” and may teach courses in either area. All other Certified Cisco Systems Instructors may only teach courses in the area of specialization for which they are certified.

Note Submit questions concerning instructor certification to icad@external.cisco.com.

Classroom Reference Materials

These items should be available for the learner during the course:

- Student Guide
- Lab Guide

Class Environment

This information describes recommended class size and classroom setup:

- Class size is based upon the number of pods in the lab setup and the number of learners per pod.
- Suggested ratio per instructor is eight pods with two learners per pod.
- Suggested access to the lab is through the Internet.
- Each pod will need a PC with Internet access.
- Third-party software will need to be installed on the PCs (see the Lab Setup section for details).

- The instructor should have access to a PC and projection system capable of projecting PowerPoint presentations.
- The instructor should have access to either a whiteboard or some other method of free-form presentation.

Course Flow

This is the *suggested* course schedule. You may make adjustments based on the skills, knowledge, and preferences of the learners in attendance. The presentation of all topics is optional for *noncertification offerings*, but you are encouraged to use them because they are designed to reinforce the lesson concepts and ensure that learners apply some of the concepts.

Day 1: Course Overview and Building a Simple Network

8:00–8:30 (0800–0830)	Course Overview
8:30–8:45 (0830–0850)	Exploring the Functions of Networking
8:45–9:15 (0850–0915)	Securing the Network
9:15–9:25 (0915–0925)	**Break**
9:25–10:00 (09:25–1000)	Understanding the Host-to-Host Communications Model
10:00–10:50 (1000–1050)	Understanding the TCP/IP Internet Layer
10:50–11:00 (1050–1100)	**Break**
11:00–11:25 (1100–1125)	Understanding the TCP/IP Transport Layer
11:25–12:00 (1125–1200)	Exploring the Packet Delivery Process
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:10 (1300–1310)	Lab 1-1: Using Windows Applications as Network Tools
1:10–1:30 (1310–1330)	Lab 1-2: Observing the TCP Three-Way Handshake
1:30–1:50 (1330–1350)	Lab 1-3: Observing Extended PC Network Information
1:50–2:00 (1350–1400)	**Break**
2:00–2:20 (1400–1420)	Understanding Ethernet
2:20–2:35 (1420–1435)	Connecting to an Ethernet LAN
2:35–3:10 (1435–1510)	Module Summary
3:10–3:20 (1510–1520)	**Break**
3:20–3:35 (1520–1535)	Understanding the Challenges of Shared LANs
3:35–3:55 (1535–1555)	Solving Network Challenges with Switched LAN Technology
3:55–4:35 (1555–1635)	Exploring the Packet Delivery Process

4:35–5:00 (1635–1700)	Operating Cisco IOS Software
5:00 (1700)	Day ends

Day 2: Ethernet LANs and WLANs

8:00–8:45 (0800–0845)	Day 1 Review
8:45–9:40 (0845–0940)	Starting a Switch
9:40–9:50 (0940–0950)	**Break**
9:50–10:20 (0950–1020)	Lab 2-1: Connecting to Remote Lab Equipment
10:20–10:50 (1020–1050)	Lab 2-2: Performing Switch Startup and Initial Configuration
10:50–11:00 (1050–1100)	**Break**
11:00–11:30 (1100–1130)	Understanding Switch Security
11:30–12:00 (1130–1200)	Lab 2-3: Enhancing the Security of Initial Switch Configuration
12:00–1:00 (1200–1300)	**Lunch**
1:00:1:30 (1300–1330)	Lab 2-4: Operating and Configuring a Cisco IOS Device
1:30–2:00 (1330–1400)	Maximizing the Benefits of Switching
2:00–2:10 (1400–1410)	**Break**
2:10–2:40 (1410–1440)	Troubleshooting Switch Issues
2:40–3:00 (1440–1500)	Module Summary
3:00–3:10 (1500–1510)	**Break**
3:10–3:50 (1510–1550)	Exploring Wireless Networking
3:50–4:10 (1550–1610)	Understanding WLAN Security
4:10–4:20 (1610–1620)	**Break**
4:30–4:50 (1630–1650)	Implementing a WLAN
4:50–5:00 (1650–1700)	Module Summary
5:00 (1700)	**Day ends**

Day 3: LAN Connections

8:00–8:20 (0800–0820)	Exploring the Functions of Routing
8:20–8:40 (0820–0840)	Understanding Binary Basics
8:40–8:50 (0840–0850)	**Break**
8:50–9:45 (0850–0945)	Constructing a Network Addressing Scheme
9:45–9:55 (0945–0955)	**Break**
9:55–11:15 (0955–1115)	Labs 4-1 through 4-4: Subnet Exercise
11:15–11:25 (1115–1125)	**Break**
11:25–11:40 (1125–1140)	Starting a Cisco Router
11:40–12:00 (1140–1200)	Configuring a Cisco Router
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:20 (1300–1320)	Lab 4-5: Initial Router Startup
1:20–1:50 (1320–1350)	Lab 4-6: Initial Router Configuration
1:50–2:00 (1350–1400)	**Break**
2:00–2:30 (1400–1430)	Exploring the Packet Delivery Process
2:30–2:40 (1430–1440)	Understanding Cisco Router Security
2:40–3:00 (1440–1500)	Lab 4-7: Enhancing the Security of Initial Router Configuration
3:00–3:10 (1500–1510)	**Break**
3:10–3:20 (1510–1520)	Using Cisco SDM
3:20–3:35 (1520–1535)	Using a Cisco Router as a DHCP Server
3:35–4:05 (1535–1605)	Lab 4-8: Using Cisco SDM to Configure DHCP Server Function
4:05–4:15 (1605–1615)	**Break**
4:15–4:25 (1615–1625)	Accessing Remote Devices
4:25–4:55 (1625–1655)	Lab 4-9: Managing Remote Access Sessions
4:55–5:00 (1655–1700)	Module Summary

5:00 (1700)	**Day ends**

Day 4: LAN Connections and WANs

8:00–8:55 (0800–0855)	Understanding WAN Technologies
8:55–9:05 (0855–0905)	**Break**
09:05–10:00 (0905–1010)	Enabling the Internet Connection
10:00–10:10 (1000–1010)	**Break**
10:10–10:40 (1010–1040)	Enabling Static Routing
10:40–11:15 (1040–1115)	Lab 5-1: Connecting to the Internet
11:15–11:25 (1115–1125)	**Break**
11:25–12:00 (1125–1400)	Configuring Serial Encapsulation
12:00–1:00 (1200–1300)	**Lunch**
1:00–1:30 (1300–1330)	Lab 5-2: Connecting to the Main Office
1:30–2:30 (1330–1430)	Enabling RIP
2:30–2:40 (1430–1440)	**Break**
2:40–3:40 (1440–1540)	Lab 5-3: Enabling Dynamic Routing to the Main Office
3:40–3:50 (1540–1550)	**Break**
3:50–4:00 (1550–1600)	Module Summary
4:00–4:30 (1600–1635)	Discovering Neighbors on the Network
4:30–5:00 (16:30–1700)	Lab 6-1: Using Cisco Discovery Protocol
5:00 (1700)	**Day ends**

Day 5: Network Environment Management and Capstone Lab

8:00–8:30 (800–0820)	Managing Cisco Router Startup and Configuration
8:30–9:00 (0830–0900)	Lab 6-2: Managing Router Startup Options
9:00–9:10 (0900–0910)	**Break**
9:10–9:40 (0910–0940)	Managing Cisco Devices

9:40–10:10 (0940–1010)	Lab 6-3: Managing Cisco Devices
10:10–10:20 (1010–1020)	**Break**
10:20–12:00 (1020–1200)	Lab 6-4: Confirming the Reconfiguration of the Branch Network
12:00–1:00 (1200–1300)	**Lunch**
1:00–4:30 (1300–1630)	Lab 6-4: Confirming the Reconfiguration of the Branch Network
4:30–5:00 (1630–1700)	**Wrap-up**

High-Level Course Outline

This subtopic provides an overview of how the course is organized. The course contains these components:

- Course Introduction
- Building a Simple Network
- Ethernet LANs
- WLANs
- LAN Connections
- WAN Connections
- Network Environment Management
- Lab Guide

Detailed Course Outline

This in-depth outline of the course structure lists each module, lesson, and topic.

Course Introduction

The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

- Overview
  - — Learner Skills and Knowledge
- Course Goal and Objectives
- Course Flow
- Additional References
  - — Cisco Glossary of Terms
- Your Training Curriculum

Module 1: Building a Simple Network

This module describes how to create a simple host-to-host network and describe network components and functions.

Lesson 1: Exploring the Functions of Networking

This lesson defines the common components, purposes, and functions of a network. Upon completing this lesson, the learner will be able to meet these objectives:

- Define a network
- List the common components of a network
- Interpret network diagrams
- List major resource-sharing functions of networks and their benefits
- List four common user applications that require network access and the benefits of each
- Describe the impact of user applications on the network
- List the categories of characteristics used to describe the various network types
- Compare and contrast physical and logical topologies
- List the characteristics of a bus topology
- List the characteristics of a star and extended-star topology
- List the characteristics of a ring and dual-ring topology
- List the characteristics of a mesh and partial-mesh topology
- Describe the methods of connecting to the Internet

The lesson includes these topics:

- What Is a Network?
- Common Physical Components of a Network
- Interpreting a Network Diagram
- Resource-Sharing Functions and Benefits
- Network User Applications
- Impact of User Applications on the Network
- Characteristics of a Network
- Physical vs. Logical Topologies
- Bus Topology
- Star and Extended-Star Topologies
- Ring Topologies
- Mesh and Partial-Mesh Topologies
- Connection to the Internet

Lesson 2: Securing the Network

This lesson defines how to explain the need for a comprehensive network security policy. Upon completing this lesson, the learner will be able to meet these objectives:

- Explain how sophisticated attack tools and open networks have generated an increased need for network security and dynamic security policies
- Describe the challenge of balancing network security needs against e-business processes, legal issues, and government policies
- Describe network adversaries, hacker motivations, and classes of attack
- Describe how to mitigate common threats to Cisco routers and switches

The lesson includes these topics:

- Need for Network Security
- Balancing Network Security Requirements
- Adversaries, Adversary Motivations, and Classes of Attack
- Mitigating Common Threats

Lesson 3: Understanding the Host-to-Host Communications Model

This lesson defines how to describe the layers of the OSI model and describe how to classify devices and their functions according to their layer in the OSI model. Upon completing this lesson, the learner will be able to meet these objectives:

- Identify the requirements of the host-to-host communication module
- Define the purpose of the OSI reference model
- Define the characteristics, functions, and purposes of each of the OSI layers
- Describe the process of encapsulation and de-encapsulation
- Describe how peer-to-peer communication works
- List the purposes and functions of the TCP/IP suite in data communications

The lesson includes these topics:

- Understanding Host-to-Host Communications
- The OSI Reference Model
- The OSI Model Layers and Their Functions
- Encapsulation and De-Encapsulation
- Peer-to-Peer Communication
- TCP/IP Suite

Lesson 4: Understanding the TCP/IP Internet Layer

This lesson defines how to manage IP addresses and to map between IP addresses and MAC addresses. Upon completing this lesson, the learner will be able to meet these objectives:

- List the characteristics of the Internet protocol
- Describe the components of an IPv4 address

- Describe the structure of an IPv4 address
- Describe the classes of IP addresses
- Describe reserved IP addresses
- Compare public and private IP addresses
- Define the function of DHCP in IP addressing
- Define the function of DNS in IP addressing
- Identify common host tools to determine the IP address of a host

The lesson includes these topics:

- Internet Protocol
- IP Addressing
- IP Address Fields
- IP Address Classes
- Reserved IP Addresses
- Public and Private IP Addresses
- Dynamic Host Configuration Protocol
- Domain Name System
- Using Common Host Tools to Determine the IP Address of a Host

The lesson includes these activities:

- Lab 1-1: Using Windows Applications as Network Tools

Lesson 5: Understanding the TCP/IP Transport Layer

This lesson defines how to compare and contrast TCP/IP with the OSI model. Upon completing this lesson, the learner will be able to meet these objectives:

- Explain the purpose and functions of the transport layer
- Contrast connection-oriented transport with connectionless transport
- List the characteristics of UDP
- List the characteristics of TCP
- List common applications provided by TCP/IP
- Describe how the protocol stack maps Layer 3 to Layer 4
- Describe how the protocol stack maps Layer 4 to applications
- Order the steps of the initialization of a TCP connection
- Describe the reasons for and the mechanics of flow control
- Order the steps in an acknowledgment sequence
- Define the function of windowing
- Define sequence and acknowledgment numbers

The lesson includes these topics:

- Transport Layer Functions
- Reliable vs. Best–Effort
- UDP
- TCP
- TCP/IP Applications
- Mapping Layer 3 to Layer 4
- Mapping Layer 4 to Applications
- Establishing a Connection with a Peer System
- Flow Control
- Acknowledgment
- Windowing
- TCP Sequence Number and Acknowledgment Numbers

The lesson includes these activities:

- Lab 1-2: Observing the TCP Three-Way Handshake

Lesson 6: Exploring the Packet Delivery Process

This lesson defines how a host-to-host connection is made and maintained. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe Layer 1 devices and their function
- Describe Layer 2 devices and their function
- Describe Layer 2 addressing
- Describe Layer 3 devices and their function
- Describe Layer 3 addressing
- Describe mapping Layer 2 addressing to Layer 3 addressing
- Describe the ARP table
- Describe packet delivery (host-to-host)
- Describe the function of the default gateway
- Use common host tools to determine the path between two hosts across a network

The lesson includes these topics:

- Layer 1 Devices and Their Function
- Layer 2 Devices and Their Function
- Layer 2 Addressing
- Layer 3 Devices and Their Function
- Layer 3 Addressing
- Mapping Layer 2 Addressing to Layer 3 Addressing
- ARP Table
- Host-to-Host Packet Delivery
- Function of the Default Gateway
- Using Common Host Tools to Determine the Path Between Two Hosts Across a Network

The lesson includes these activities:

- Lab 1-3: Observing Extended PC Network Information

Lesson 7: Understanding Ethernet

This lesson defines how to list the characteristics and benefits of a LAN, including its components and their related functions. Upon completing this lesson, the learner will be able to meet these objectives:

- Define a LAN
- Identify the components of a LAN
- List the functions of a LAN
- Describe LAN sizes
- Describe the evolution of Ethernet (IEEE 802.3)
- Describe the standards that govern Ethernet
- Define how CSMA/CD operates
- Identify the fields of an Ethernet frame and explain their functions
- List the characteristics of each type of Ethernet frame addressing
- Define the purpose and components of an Ethernet address
- Define the hexadecimal structure and function of MAC addresses in an Ethernet LAN

The lesson includes these topics:

- Definition of a LAN
- Components of a LAN
- Functions of a LAN
- How Big Is a LAN?
- Ethernet
- Ethernet LAN Standards

- The Role of CSMA/CD in Ethernet
- Ethernet Frames
- Ethernet Frame Addressing
- Ethernet Addresses
- MAC Addresses and Binary-Hexadecimal Numbers

Lesson 8: Connecting to an Ethernet LAN

This lesson defines how to list the types and functions of the connection components of an Ethernet LAN. Upon completing this lesson, the learner will be able to meet these objectives:

- List the functions of a NIC in an Ethernet LAN
- List the connection requirements for an Ethernet LAN
- Define the types of Ethernet LAN connection media
- List the characteristics of an unshielded twisted-pair cable
- Recognize the differences between straight-through and crossover cables, and explain the appropriate uses for each

The lesson includes these topics:

- Ethernet Network Interface Cards
- Ethernet Media and Connection Requirements
- Connection Media
- Unshielded Twisted-Pair Cable
- UTP Implementation

Module 2: Ethernet LANs

This module describes how to expand an Ethernet LAN by adding a hub.

Lesson 1: Understanding the Challenges of Shared LANs

This lesson defines how to identify the issues related to increasing traffic on an Ethernet LAN. Upon completing this lesson, the learner will be able to meet these objectives:

- Define Ethernet LAN segments and their distance limitations
- List the characteristics and functions of a hub in an Ethernet LAN
- Define collisions on a LAN and list the conditions that produce them
- Define collision domains in an Ethernet LAN

The lesson includes these topics:

- Ethernet LAN Segments
- Extending a LAN Segment
- Collisions
- Collision Domains

Lesson 2: Solving Network Challenges with Switched LAN Technology

This lesson defines how to identify switched LAN technology solutions to Ethernet networking issues. Upon completing this lesson, the learner will be able to meet these objectives:

- Identify the typical causes of network congestion on an Ethernet LAN
- List the characteristics and functions of a bridge in alleviating network congestion
- List the characteristics and functions of a switch
- Compare the network performance of a switch to the network performance of a bridge
- List the three functions of a switch
- Describe how switching works
- Describe how LANs today use switching technology

The lesson includes these topics:

- Typical Causes of Network Congestion
- Bridges—Early Solutions to Network Congestion
- Switches
- Switches versus Bridges
- How Switches Segment the Ethernet Network
- Switching in Action
- LANs Using Switched Technology

Lesson 3: Exploring the Packet Delivery Process

This lesson defines how a host-to-host connection is made and maintained. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe Layer 2 addressing
- Describe Layer 3 addressing
- Describe packet delivery (host-to-host)

The lesson includes these topics:

- Layer 2 Addressing
- Layer 3 Addressing
- Host-to-Host Packet Delivery

Lesson 4: Operating Cisco IOS Software

This lesson defines how to set up console connections between Cisco network devices and a terminal. Upon completing this lesson, the learner will be able to meet these objectives:

- List the features and functions of Cisco IOS Software in relation to enterprise network considerations
- Describe the initial startup for Cisco network devices
- Describe external configurations for Cisco network devices

- Define the features of the Cisco IOS CLI
- Describe how to start an EXEC session and change EXEC modes
- Identify the online help functions associated with the device CLI
- Describe the enhanced editing functions of the Cisco IOS CLI
- Use the device command history feature of the CLI

The lesson includes these topics:

- Cisco IOS Software Features and Functions
- Configuring Network Devices
- External Configuration Sources
- Cisco IOS CLI Functions
- Entering the EXEC Modes
- Keyboard Help in the CLI
- Enhanced Editing Commands
- Command History

Lesson 5: Starting a Switch

This lesson defines how to start an access layer switch and use the CLI to configure and to monitor the switch. Upon completing this lesson, the learner will be able to meet these objectives:

- Start up a Cisco IOS switch
- Identify the conditions reflected by the LEDs on Cisco IOS switches
- Describe the initial boot output from a Cisco IOS switch
- Log in to a Cisco IOS switch
- Configure a Cisco IOS switch from the command line
- Verify the initial switch operation
- Use the appropriate **show** command for MAC address table management

The lesson includes these topics:

- Physical Startup of the Catalyst Switch
- Switch LED Indicators
- Viewing Initial Bootup Output from the Switch
- Logging In to the Switch
- Configuring a Switch from the Command Line
- Showing the Switch Initial Startup Status
- MAC Address Table Management

The lesson includes these activities:

- Lab 2-1: Connecting to Remote Lab Equipment

- Lab 2-2: Performing Switch Startup and Initial Configuration
- Lab 2-4: Operating and Configuring a Cisco IOS Device

Lesson 6: Understanding Switch Security

This lesson defines how to implement a basic configuration for a Cisco switch. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe how to mitigate hardware, environmental, electrical, and maintenance-related security threats to Cisco switches and switches
- Configure password security
- Configure the Login Banner
- Describe the difference between using Telnet versus SSH for remote access
- Configure port security
- Secure unused ports

The lesson includes these topics:

- Physical and Environmental Threats
- Configuring Password Security
- Configuring the Login Banner
- Telnet vs. SSH Access
- Port Security Configuration
- Securing Unused Ports

The lesson includes these activities:

- Lab 2-3: Enhancing the Security of Initial Switch Configuration

Lesson 7: Maximizing the Benefits of Switching

This lesson defines the ways in which an Ethernet LAN can be optimized. Upon completing this lesson, the learner will be able to meet these objectives:

- List the characteristics and advantages of microsegmentation
- Compare half-duplex and full-duplex operation in an Ethernet LAN
- Identify the need for different media rates in enterprise networks and describe how this need can be satisfied in a switched Ethernet network
- Describe how loops can affect performance in a switched LAN
- Describe how STP protects against loops resulting from physical redundancy in an Ethernet LAN

The lesson includes these topics:

- Microsegmentation
- Duplex Communication
- The Need for Different Media Rates in an Enterprise Network

- Physical Redundancy in an Ethernet LAN
- Loop Resolution with Spanning Tree Protocol

Lesson 8: Troubleshooting Switch Issues

This lesson defines how to identify and resolve common switch network issues. Upon completing this lesson, the learner will be able to meet these objectives:

- Identify switch issues using a layered approach
- Identify and resolve common switched network media issues
- Identify and resolving common access port issues
- Identify and resolve common configuration issues

The lesson includes these topics:

- Using a Layered Approach
- Identifying and Resolving Media Issues
- Identifying and Resolving Common Access Port Issues
- Identifying and Resolving Common Configuration Issues

Module 3: Wireless LANs

This module describes the WLAN environment.

Lesson 1: Exploring Wireless Networking

This lesson defines how to describe the factors that affect wireless LANs and the standards that govern wireless LANs. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the business case for WLAN services
- Describe the differences between WLAN and LAN implementations
- Identify the characteristics of the radio frequency transmissions used by WLANs
- Identify the organizations that define WLAN standards
- Describe the three unlicensed bands used by ITU-R local FCC Wireless
- Compare the different IEEE 802.11 standards
- Describe Wi-Fi certification

The lesson includes these topics:

- The Business Case for WLAN Service
- Differences Between WLANs and LANs
- Radio Frequency Transmission
- Organizations that Define WLANs
- ITU-R Local FCC Wireless
- 802.11 Standards Comparison
- Wi-Fi Certification

Lesson 2: Understanding WLAN Security

This lesson defines how to describe WLAN security issues and the features available to increase WLAN security. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe common threats to WLAN services
- Describe methods of mitigating security threats to WLAN services
- Describe the evolution of WLAN security.
- Describe the wireless client association process
- Describes how IEEE 802.1X provides additional WLAN security
- Describe the modes of WPA

The lesson includes these topics:

- Wireless LAN Security Threats
- Mitigating Security Threats
- Evolution of Wireless LAN Security
- Wireless Client Association
- How 802.1X Works on WLANs
- WPA and WPA2 Modes

Lesson 3: Implementing a WLAN

This lesson defines how to describe the operation of routers in connecting multiple networks. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the IEEE 802.11 topologies
- Describe BSA WLAN service
- Describe the effect of distance and speed on WLAN service
- Describe the factors that should be considered in implementation of an access point
- Describe basic wireless implementation
- Describes the form factors to add wireless to existing laptops
- Describe how to troubleshoot common wireless issues

The lesson includes these topics:

- 802.11 Topology Building Blocks
- BSA Wireless Topology
- Wireless Topology Data Rates
- Access Point Configuration
- Steps to Implement a Wireless Network
- Wireless Clients
- Wireless Troubleshooting

Module 4: LAN Connections

This module describes the reasons for connecting networks with routers and how routed networks transmit data through networks using TCP/IP.

Lesson 1: Exploring the Functions of Routing

This lesson defines how to describe the operation of Cisco routers in connecting multiple networks. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the physical characteristics of a router and the functions of a router in the IP packet delivery process
- Describe the method used in determining the optimal path for forwarding IP packets between networks
- List the characteristics of routing tables and their function in path determination
- Match the characteristics of a static route, dynamic route, directly connected route, and default route to the appropriate route type
- List the characteristics of routing protocols that build and maintain routing tables automatically

The lesson includes these topics:

- Routers
- Path Determination
- Routing Tables
- Static, Dynamic, Directly Connected, and Default Routes
- Dynamic Routing Protocols

Lesson 2: Understanding Binary Basics

This lesson defines how to convert a decimal number into a binary number and a binary number into decimal number. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the decimal and binary number systems
- Describe the “powers of 2” process
- Convert a decimal number to a binary number
- Convert a binary number to a decimal number

The lesson includes these topics:

- Decimal and Binary Systems
- Powers of 2
- Decimal-to-Binary Conversion
- Binary-to-Decimal Conversion

The lesson includes this activity:

- Lab 4-1: Converting Decimal to Binary and Binary to Decimal

Lesson 3: Constructing a Network Addressing Scheme

This lesson describes how to describe and calculate subnet addresses. Upon completing this lesson, the learner will be able to meet these objectives:

- Define the purpose and function of a subnet
- Describe the process of computing usable subnet and host addresses
- Describe how end systems use subnet masks to locate a destination device
- Describe how routers use subnet masks to route a packet to its destination
- Describe the mechanics of subnet mask operation
- Apply subnet mask operations to Class A, B, and C IP addresses

The lesson includes these topics:

- Subnetworks
- Computing Usable Subnetworks and Hosts
- How End Systems Use Subnet Masks
- How Routers Use Subnet Masks
- Mechanics of Subnet Mask Operation
- Applying Subnet Mask Operation

The lesson includes these activities:

- Lab 4-2: Classifying Network Addressing
- Lab 4-3: Computing Usable Subnetworks and Hosts
- Lab 4-4: Calculating Subnet Masks

Lesson 4: Starting a Cisco Router

This lesson defines how to start a Cisco router and use CLI commands to configure and monitor the Cisco router. Upon completing this lesson, the learner will be able to meet these objectives:

- Start up a Cisco router
- Start the initial setup process for a Cisco router
- Log in to a Cisco router
- Show the hardware and software status of a Cisco router

The lesson includes these topics:

- Initial Startup of a Cisco Router
- Initial Setup of a Cisco Router
- Logging In to the Cisco Router
- Showing the Router Initial Startup Status

The lesson includes these activities:

- Lab 4-5: Performing Initial Router Startup

Lesson 5: Configuring a Cisco Router

This lesson defines how to implement a basic configuration for a Cisco router. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the router configuration modes
- Configure a router from the CLI
- Configure router interfaces
- Configure a router IP address
- Verify the router interface configuration

The lesson includes these topics:

- Cisco Router Configuration Modes
- Configuring a Cisco Router from the CLI
- Configuring Cisco Router Interfaces
- Configuring the Cisco Router IP Address
- Verifying the Interface Configuration

The lesson includes these activities:

- Lab 4-6: Performing Initial Router Configuration

Lesson 6: Exploring the Packet Delivery Process

This lesson defines how a host-to-host connection is made and maintained. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe Layer 2 addressing
- Describe Layer 3 addressing
- Describe host-to-host packet delivery
- Describe the use of the **show ip arp** command
- Describe the use of common Cisco IOS tools to verify connectivity

The lesson includes these topics:

- Layer 2 Addressing
- Layer 3 Addressing
- Host-to-Host Packet Delivery
- Using the **show ip arp** Command
- Using Common Cisco IOS Tools

Lesson 7: Understanding Cisco Router Security

This lesson defines how to implement a basic security configuration for a Cisco router. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe how to mitigate hardware, environmental, electrical, and maintenance-related security threats to Cisco routers
- Configure password security
- Configure the login banner
- Describe Telnet and SSH for remote access

The lesson includes these topics:

- Physical and Environmental Threats
- Configuring Password Security
- Configuring the Login Banner
- Telnet and SSH Access

The lesson includes these activities:

- Lab 4-7: Enhancing the Security of the Initial Router Configuration

Lesson 8: Using Cisco SDM

This lesson defines the features of Cisco SDM. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the features of Cisco SDM
- Explain how to use the elements of the Cisco SDM interface
- Explain the function of each of the five Cisco SDM wizards

The lesson includes these topics:

- Cisco SDM Overview
- Cisco SDM User Interface
- Cisco SDM Wizards

Lesson 9: Using a Cisco Router as a DHCP Server

This lesson defines how to configure a Cisco IOS DHCP server using Cisco SDM. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the features of DHCP
- Describe using a router as a DHCP server
- Describe how to use Cisco SDM to enable the DHCP server to function on a router
- Describe how to monitor DHCP server functions

The lesson includes these topics:

- Understanding DHCP

- Using a Cisco Router as a DHCP Server
- Using Cisco SDM to Enable the DHCP Server Function
- Monitoring DHCP Server Functions

The lesson includes these activities:

- Lab 4-8: Using Cisco SDM to Configure DHCP Server Function

Lesson 10: Accessing Remote Devices

This lesson defines how to use Cisco IOS Software tools to access a remote device. Upon completing this lesson, the learner will be able to meet these objectives:

- Use Telnet and SSH to connect to remote network devices
- Suspend and resume a Telnet session
- Close a Telnet session
- Use Cisco IOS Software commands to test connectivity

The lesson includes these topics:

- Establishing a Telnet or SSH Connection
- Suspending and Resuming a Telnet Session
- Closing a Telnet Session
- Alternate Connectivity Tests

The lesson includes these activities:

- Lab 4-9: Managing Remote Access Sessions

Module 5: WAN Connections

This module describes the characteristics, functions, and components of a WAN.

Lesson 1: Understanding WAN Technologies

Upon completing this lesson, the learner will be able to meet these objectives:

- List the functions and characteristics of a WAN
- List the business needs for WANs
- Compare WANs to LANs
- Describe how WAN protocols operate in relation to the OSI reference model
- List the hardware devices that typically function in connecting to a WAN and define their functions
- Describe the cabling that is available for WAN connections
- Define the role of routers for WAN access
- List the major protocols that operate in a WAN environment
- List the major types of WAN access communication link options

The lesson includes these topics:

- What Is a WAN?
- Why Are WANs Necessary?
- How Is a WAN Different from a LAN?
- WAN Access and the OSI Reference Model
- WAN Devices
- WAN Cabling
- The Role of Routers in WANs
- WAN Data-Link Protocols
- WAN Communication Link Options

Lesson 2: Enabling the Internet Connection

This lesson defines how to configure Internet access using the DHCP client, NAT, and PAT on Cisco IOS routers. Upon completing this lesson, the learner will be able to meet these objectives:

- Define the functions of a packet-switched WAN communication link
- List the characteristics and functions of DSL
- List the characteristics and functions of cable-based WANs
- Describe the evolution and the function of the global Internet
- Describe the process of obtaining an interface address from a DHCP server
- Describe the features of NAT and PAT on Cisco routers
- Describe using static and dynamic translation to translate inside source addresses
- Use Cisco SDM to configure the DHCP client and PAT by overloading an inside global address
- Use Cisco SDM to verify that the DHCP client is operating as expected
- Use Cisco IOS commands to verify that NAT and PAT are operating as expected

The lesson includes these topics:

- Packet-Switched Communication Links
- Digital Subscriber Line
- Cable
- Global Internet: The Largest WAN
- Obtaining an Interface Address from a DHCP Server
- Introducing NAT and PAT
- Translating Inside Source Addresses
- Configuring the DHCP Client and PAT
- Verifying the DHCP Client Configuration
- Verifying the NAT and PAT Configuration

Lesson 3: Enabling Static Routing

This lesson defines the operation, benefits, and limitations of static and dynamic routing. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the basic characteristics of IP static and dynamic routing
- Explain the differences between static and dynamic routing
- Configure static routes on Cisco routers
- Configure default route forwarding
- Verify static route configurations

The lesson includes these topics:

- Routing Overview
- Static and Dynamic Route Comparison
- Static Route Configuration
- Default Route Forwarding Configuration
- Static Route Configuration Verification

The lesson includes these activities:

- Lab 5-1: Connecting to the Internet

Lesson 4: Configuring Serial Encapsulation

This lesson defines how to configure serial ports for PPP. Upon completing this lesson, the learner will be able to meet these objectives:

- Define the functions and characteristics of circuit-switched WAN communication links
- Define the characteristics and functions of the PSTN
- Define the functions and characteristics of point-to-point communication links
- Define the characteristics of HDLC
- Explain how to configure HDLC encapsulation on a serial port
- Define the characteristics of PPP and describe how it is enabled on a serial interface
- Verify HDLC and PPP configurations
- Define the characteristics of Frame Relay
- Define the characteristics of ATM

The lesson includes these topics:

- Circuit-Switched Communication Links
- Public Switched Telephone Network
- Point-to-Point Communication Links
- High-Level Data-Link Control Protocol
- Configuring HDLC Encapsulation
- Point-to-Point Protocol

- Serial Encapsulation Configuration Verification
- Frame Relay
- ATM and Cell Switching

The lesson includes these activities:

- Lab 5-2: Connecting to the Main Office

Lesson 5: Enabling RIP

This lesson defines the operation, benefits, and limitations of static and dynamic routing. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the purpose, types, and classes of dynamic routing protocols
- Describe the different classes of routing protocols
- Describe how a distance vector routing protocol selects routes and maintains routing information
- Describe the features of RIP
- Describe the differences between RIPv1 and RIPv2
- Describe the tasks required to enable a dynamic routing protocol on a Cisco router
- Describe the configuration tasks needed to enable basic RIP routing on a Cisco router
- Use the **show** commands to verify the RIP configuration
- Describe the use of the **debug ip rip** command

The lesson includes these topics:

- Dynamic Routing Protocol Overview
- Classless vs. Classful Routing
- Distance Vector Route Selection
- RIP Features
- RIPv1 and RIPv2 Comparison
- Dynamic Routing Configuration Tasks
- RIP Configuration
- RIP Configuration Verification
- RIP Configuration Troubleshooting

The lesson includes these activities:

- Lab 5-3: Enabling Dynamic Routing to the Main Office

Module 6: Network Environment Management

This module describes how to manage devices on a network.

Lesson 1: Discovering Neighbors on the Network

This lesson defines how to use the CLI to discover neighbors on the network. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the purpose and function of the Cisco Discovery Protocol
- Describe the information provided by Cisco Discovery Protocol
- Enable and disable Cisco Discovery Protocol
- Determine the host names and addresses of neighboring Cisco devices using Cisco Discovery Protocol
- Monitor and maintain information about neighboring Cisco devices using Cisco Discovery Protocol
- Use information gathered using Cisco Discovery Protocol to create a network map of the environment

The lesson includes these topics:

- Cisco Discovery Protocol
- Information Obtained with Cisco Discovery Protocol
- Implementation of Cisco Discovery Protocol
- Using the **show cdp neighbors** Command
- Monitoring and Maintaining Cisco Discovery Protocol
- Creating a Network Map of the Environment

The lesson includes these activities:

- Lab 6-1: Using Cisco Discovery Protocol

Lesson 2: Managing Cisco Router Startup and Configuration

This lesson defines how to manage startup and configuration of a Cisco router. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the router boot sequence and explain how to verify that the router booted correctly
- Identify the internal components of Cisco routers
- Describe the process for locating the Cisco IOS image
- Display and change the boot information in the configuration register

The lesson includes these topics:

- Stages of the Router Power-On Boot Sequence
- Internal Router Components
- How a Cisco Device Locates and Loads Cisco IOS Image and Configuration Files
- Configuration Register

The lesson includes these activities:

- Lab 6-2: Managing Router Startup Options

Lesson 3: Managing Cisco Devices

This lesson defines how to manage Cisco IOS images, configuration files, and devices on the network. Upon completing this lesson, the learner will be able to meet these objectives:

- Describe the file systems used by a Cisco router
- Manage Cisco IOS image files to maintain accessible Cisco IOS images
- Manage device configuration files to reduce device downtime
- Use the **copy** command to move configurations
- Use troubleshooting commands and processes to minimize any potentially adverse impact on Cisco devices

The lesson includes these topics:

- Cisco IOS File System and Devices
- Managing Cisco IOS Images
- Managing Device Configuration Files
- Cisco IOS **copy** Command
- Using **show** and **debug** Commands on Operational Cisco Devices

The lesson includes these activities:

- Lab 6-3: Managing Cisco Devices

Capstone Lab: Network Environment Management

In this activity, learners will assume that they are taking over the reconfiguration of a branch network from an administrator who has not completed the configuration. In fact, there may be misconfiguration of some of the settings. They will use their knowledge and experience from the earlier labs to complete reconfiguration, correction, and testing.

Upon completing this lesson, the learner will be able to meet these objectives:

- Complete the reconfiguration of their assigned workgroup switch using information provided in worksheet sheet format
- Complete the reconfiguration of their workgroup router using information provided in worksheet format
- Perform tests to validate that their final configuration meets the new topology information.

The lesson includes this activity:

- Lab 6-4: Confirming the Reconfiguration of the Branch Network

Course Evaluations

Cisco uses a post-course evaluation system, Metrics That Matter (MTM), for its instructor-led courses. The instructor must ensure that each learner is aware of the confidential evaluation process and that all learners submit an evaluation for each course. There are two options for learners to complete the evaluation.

For Classes with Internet Access

A URL will be made available, specific to each Cisco Learning Partner. Obtain the URL from your MTM system administrator before the last day of class.

1. Upon completion of the course, instruct the learners to enter the URL into their browser.
2. Make sure that the learners input their e-mail address (used only for a follow-up evaluation).

Note Sixty days following a learning event, learners will receive a brief follow-up evaluation, and, again, responses will be kept confidential. E-mail addresses will not be used for marketing purposes. (If learners do not have e-mail addresses, they may type in a "dummy" address.)

3. Instruct the learners to select the appropriate course from the drop-down list.
4. Instruct the learners to complete the course evaluation and click Submit one time only.
5. Advise the learners to wait for "Thank you" to appear on the screen before leaving.

For Classes Without Internet Access

A paper-based version of the post-course evaluation is available. Your MTM system administrator can provide you with copies.

1. Distribute paper-based evaluations at the beginning of the last day of class.
2. Instruct the learners to complete the survey only after completing the course.
3. Collect the evaluations and submit them to your MTM system administrator.

To View Evaluation Results

To view your post-course evaluation results:

1. Go to http://www.metricsthatmatter.com/client. (Reminder: All data is confidential; you will see only your own data.)
2. Log in using your ID and the password sent to you from MTM or provided by your company MTM system administrator to ensure confidentiality.
3. Choose Menu Option – Learner Evaluation Reports:
   - — Evaluation Retrieval Tool
   - — Class Evaluation Summary Report
4. Search for and select the appropriate class.

Lab Setup

Overview

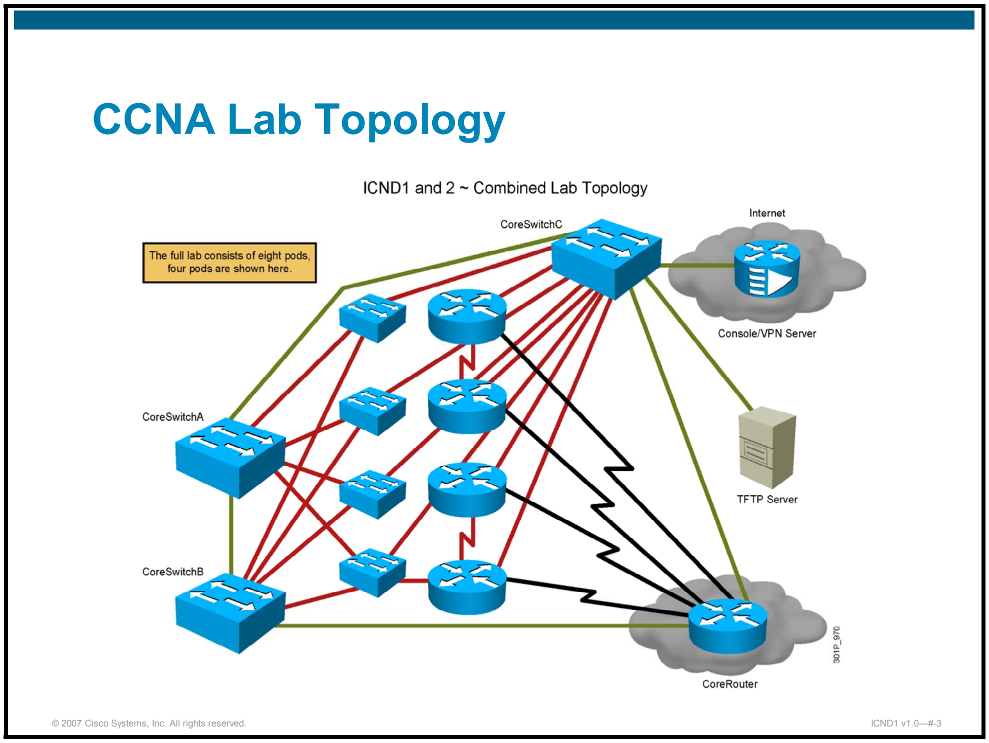
The purpose of the “Lab Setup” section is to assist in the setup and configuration of the training equipment for ICND1. This section includes these topics:

- Lab Topology
- Hardware and Software Requirements
- Workstation Configuration
- Lab Equipment Configuration
- General Lab Setup
- Lab 1-1: Using Windows Applications as Network Tools
- Lab 1-2: Observing the TCP Three-Way Handshake
- Lab 1-3: Observing Extended PC Network Information
- Lab 2-1: Connecting to Remote Lab Equipment
- Lab 2-2: Performing Switch Startup and Initial Configuration
- Lab 2-3: Enhancing the Security of Initial Switch Configuration
- Lab 2-4: Operating and Configuring a Cisco IOS Device
- Lab 4-1: Converting Decimal to Binary and Binary to Decimal
- Lab 4-2: Classifying Network Addressing
- Lab 4-3: Computing Usable Subnetworks and Hosts
- Lab 4-4: Calculating Subnet Masks
- Lab 4-5: Performing Initial Router Startup
- Lab 4-6: Performing Initial Router Configuration
- Lab 4-7: Enhancing the Security of the Initial Router Configuration
- Lab 4-8: Using Cisco SDM to Configure DHCP Server Function
- Lab 4-9: Managing Remote Access Sessions
- Lab 5-1: Connecting to the Internet
- Lab 5-2: Connecting to the Main Office

- Lab 5-3: Enabling Dynamic Routing to the Main Office
- Lab 6-1: Using Cisco Discovery Protocol
- Lab 6-2: Managing Router Startup Options
- Lab 6-3: Managing Cisco Devices
- Lab 6-4: Confirming the Reconfiguration of the Branch Network
- Configuration Files Summary
- Lab Activity Solutions
- Teardown and Restoration
- Delta Information for *Interconnecting Cisco Networking Devices* v1.0

Lab Topology

This topic describes the lab topology for ICND1 v1.0.

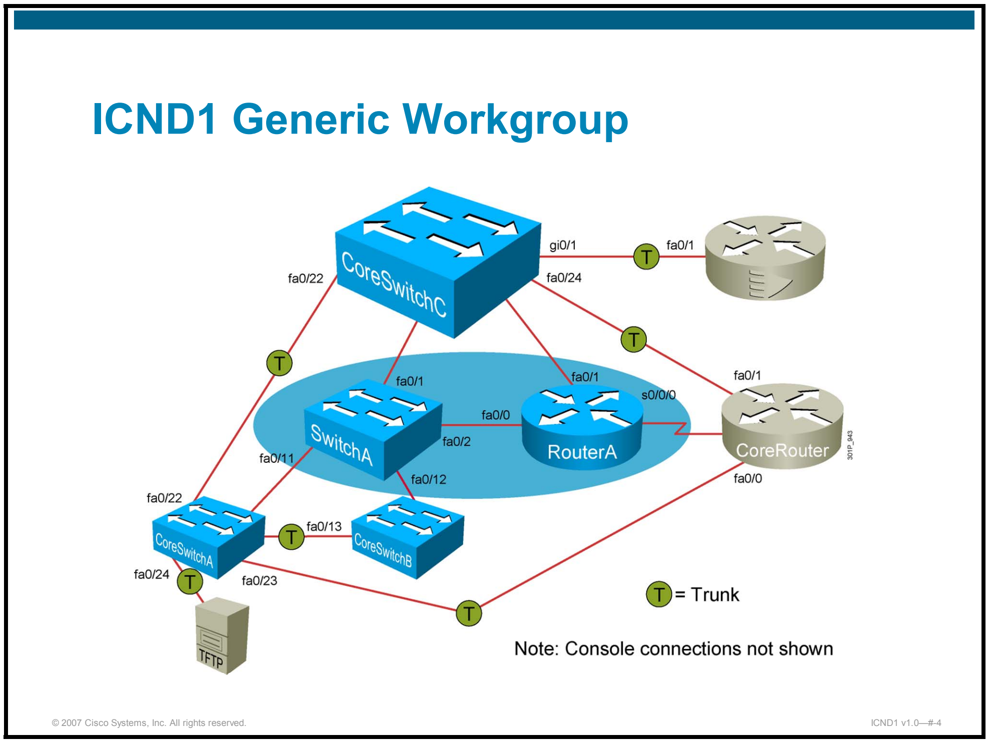


CCNA Lab Topology

ICND1 and 2 ~ Combined Lab Topology
The full lab consists of eight pods, four pods are shown here.
CoreSwitchC
Internet
Console/VPN Server
CoreSwitchA
TFTP Server
CoreSwitchB
CoreRouter
301P_970

ICND1 v1.0—#-3

The lab topologies for ICND1 and ICND2 are based on a common lab setup. In ICND1, all the core devices are actively used, but the serial line *between* workgroup routers is *not* used.



ICND1 Generic Workgroup

ICND1 v1.0—#-4

Hardware and Software Requirements

Equipment List

These tables list the recommended equipment to support the lab activities. These tables assume a class size of 16 learners.

Hardware Equipment List

	Mfr.	Part Number	Total Qty.
Learner Pod Equipment—2 Students per Pod—8 Pods Total per Class			
Catalyst 2960 Series Switch	Cisco	WS-2960-24TT-L	8
Cisco 2811 Integrated Services Router	Cisco	CISCO2811	8
2-Port Serial WIC	Cisco	WIC-2T	8
Cables DTE	Cisco	CAB-SS-X21MT	12
Cables DCE	Cisco	CAB-SS-X21FC	4
Microsoft Windows PC	Varies	N/A	8
Common Equipment—Supports 8 Pods—1 Set per Class			
Catalyst 2960 Series Switch (CoreSwitchA/B/C)	Cisco	WS-2960-24TT-L	3
Cisco 2811 Integrated Services Router (CoreRouter)	Cisco	CISCO 2811	1
8-Port Asynchronous Serial Network Module	Cisco	NM-8A/S	1
Cables DCE	Cisco	CAB-X21FC	8
2-Port Serial WIC	Cisco	WIC-2T	1
Cables DTE	Cisco	CAB-SS-X21MT	1
Cables DCE	Cisco	CAB-SS-X21FC	1
Cisco 2811 Integrated Services Router (VPN/Console server)	Cisco	CISCO2811	1
16-Port Asynchronous Module	Cisco	NM-16A	1
Cables for NM-16A	Cisco	CAB-OCTAL-ASYNC	2
8-Port Async HWIC	Cisco	HWIC8A	1
High Density 8-port EIA-232 Async Cable	Cisco	CAB-HD-ASYNC	1
Other Required Equipment			
A TFTP server is required.	Generic	N/A	1
Windows-based PC, 802.1Q Ethernet adapter PCI (TFTP server)	Linksys	EG1032	1

Software List

The software listed in the following table is suggested for this learning product.

Description	Mfr.	Part Number	Qty.
C2960-LANBASEK9-M, Version 12.2	Cisco	TBD	1 per device
C2800NM-ADVIPSERVICESK9-M, Version 12.4	Cisco	TBD	1 per device
PCs: Windows 2000/XP	Microsoft	N/A	1 per PC
PCs: Cisco VPN Client Software	Cisco	N/A	8 (download from Cisco.com)
Wireshark Packet Sniffer	http://www.wireshark.org/	N/A	8 (on Course CD)
PuTTY Term emulator	http://www.putty.nl/	N/A	8 (on Course CD)
TFTP32	http://tftpd32.jounin.net/	N/A	http://tftpd32.jounin.net/

Note Note the exact version number of the Cisco IOS software cannot be predicted, as version availability changes over time. Therefore you should select the latest maintenance version for the Cisco IOS package indicated.

Workstation Configuration

These instructions describe how to set up the lab when workstations are required.

Step 1 A Windows-based PC is required.

Step 2 Download and install Cisco VPN Client software, and provide a shortcut on the desktop.

Step 3 Copy VPN client profiles from the instructor CD to VPN Client profiles directory.

Step 4 Install Wireshark sniffer software from the instructor CD, and provide a shortcut on the desktop.

Step 5 Install PuTTY terminal emulation software from the instructor CD, and provide a shortcut on the desktop.

Step 6 Locate the network properties of the Ethernet interface adapter that will be used to access the remote lab, and create a shortcut on the desktop.

Lab Equipment Configuration

This equipment configuration information is necessary for initial setup of the lab configuration.

- Save in startup-config of CoreSwitchA configuration file “i1-coreswa-all.txt”
- Save in startup-config of CoreSwitchB configuration file “i1-coreswb-all.txt”
- Save in startup-config of CoreSwitchC configuration file “i1-coreswc-startup.txt”
- Save in startup-config of CoreRouter using configuration file “i1-corero-startup.txt”
- Save in startup-config of VPNTS configuration file vpnts-all.txt

Note The VPNTS configuration is used unaltered for ICND1 or ICND2 labs.

Initial Lab Build

The following tables contain the information required to interconnect the ICND1 and ICND2 lab equipment.

Note The username and password, when required, are **instructor** and **icndinstructor**, and the enable password on the core devices is **icndinstructor.**

Table 1: Core Devices

Device Name	Device Name Abbreviation	Assigned Pod	Interface	Network Address /24	Additional Information
CoreRouter	corero	N/A	N/A	10.1.1.3	See Table10
CoreSwitchA	coreswa	N/A	N/A	10.1.1.2	See Table5
CoreSwitchB	coreswb	N/A	N/A	10.1.1.4	See Table 6
CoreSwitchC	coreswc	N/A	N/A	10.1.1.5	See Table 7
VPNTS	vpnts	N/A	N/A	10.1.1.100	See Table 8/9
TFTP Server	-	N/A	N/A	10.1.1.1	-

Table 2: Workgroup Devices—IP addresses

Device Name	Device Name Abbreviation	Assigned Pod	Interface	Network Address /24	Additional Information
RouterA	N/A	A	fa0/0	10.2.2.3	
RouterA	N/A	A	fa0/1	172.31.241.x	DHCP supplied
RouterA	N/A	A	s0/0/0	10.140.1.2	
SwitchA	N/A	A	VLAN1	10.2.2.11	
RouterB	N/A	B	fa0/0	10.3.3.3	
RouterB	N/A	B	fa0/1	172.31.242.x	DHCP supplied
RouterB	N/A	B	s0/0/0	10.140.2.2	
SwitchB	N/A	B	VLAN1	10.3.3.11	
RouterC	N/A	C	fa0/0	10.4.4.3	
RouterC	N/A	C	fa0/1	172.31.243.x	DHCP supplied
RouterC	N/A	C	s0/0/0	10.140.3.2	
SwitchC	N/A	C	VLAN1	10.4.4.11	
RouterD	N/A	D	fa0/0	10.5.5.3	
RouterD	N/A	D	fa0/1	172.31.244.x	DHCP supplied
RouterD	N/A	D	s0/0/0	10.140.4.2	
SwitchD	N/A	D	VLAN1	10.5.5.11	
RouterE	N/A	E	fa0/0	10.6.6.3	
RouterE	N/A	E	fa0/1	172.31.245.x	DHCP supplied
RouterE	N/A	E	s0/0/0	10.140.5.2	
SwitchE	N/A	E	VLAN1	10.6.6.11	
RouterF	N/A	F	fa0/0	10.7.7.3	
RouterF	N/A	F	fa0/1	172.31.246.x	DHCP supplied
RouterF	N/A	F	s0/0/0	10.140.6.2	
SwitchF	N/A	F	VLAN1	10.7.7.11	
RouterG	N/A	G	fa0/0	10.8.8.3	
RouterG	N/A	G	fa0/1	172.31.247.x	DHCP supplied
RouterG	N/A	G	s0/0/0	10.140.7.2	
SwitchG	N/A	G	VLAN1	10.8.8.11	
RouterH	N/A	H	fa0/0	10.9.9.3	
RouterH	N/A	H	fa0/1	172.31.248.x	DHCP supplied
RouterH	N/A	H	s0/0/0	10.140.8.2	
SwitchH	N/A	H	VLAN1	10.9.9.11	

Table 3: Workgroups A–D Cabling

Device	Interface	Remote Device	Interface	Remarks
RouterA	fa0/0	SwitchA	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/2	ST
	s0/0/0	CoreRouter	s1/0	DTE
	s0/1	RouterB	s0/1	DTE
SwitchA	fa0/1	CoreSwitchC	fa0/1	XO
	fa0/2	RouterA	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/1	XO
	fa0/12	CoreSwitchB	fa0/1	XO
RouterB	fa0/0	SwitchB	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/4	ST
	s0/0/0	CoreRouter	s1/1	DTE
	s0/1	RouterA	s0/1	DCE
SwitchB	fa0/1	CoreSwitchC	fa0/3	XO
	fa0/2	RouterB	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/2	XO
	fa0/12	CoreSwitchB	fa0/2	XO
RouterC	fa0/0	SwitchC	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/6	ST
	s0/0/0	CoreRouter	s1/2	DTE
	s0/1	RouterD	s0/1	DTE
SwitchC	fa0/1	CoreSwitchC	fa0/5	XO
	fa0/2	RouterC	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/3	XO
	fa0/12	CoreSwitchB	fa0/3	XO
RouterD	fa0/0	SwitchD	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/8	ST
	s0/0/0	CoreRouter	s1/3	DTE
	s0/1	RouterC	s0/1	DCE
SwitchD	fa0/1	CoreSwitchC	fa0/7	XO
	fa0/2	RouterD	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/4	XO
	fa0/12	CoreSwitchB	fa0/4	XO

Note ST = straight RJ-45, XO = crossover RJ-45

Table 4: Workgroups E–H Cabling

Device	Interface	Remote Device	Interface	Remarks
RouterE	fa0/0	SwitchE	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/10	ST
	s0/0/0	CoreRouter	s1/4	DTE
	s0/1	RouterF	s0/1	DTE
SwitchE	fa0/1	CoreSwitchC	fa0/9	XO
	fa0/2	RouterE	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/5	XO
	fa0/12	CoreSwitchB	fa0/5	XO
RouterF	fa0/0	SwitchF	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/12	ST
	s0/0/0	CoreRouter	s1/5	DTE
	s0/1	RouterE	s0/1	DCE
SwitchF	fa0/1	CoreSwitchC	fa0/11	XO
	fa0/2	RouterF	fa0/0	STR
	fa0/11	CoreSwitchA	fa0/6	XO
	fa0/12	CoreSwitchB	fa0/6	XO
RouterG	fa0/0	SwitchG	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/14	ST
	s0/0/0	CoreRouter	s1/6	DTE
	s0/1	RouterH	s0/1	DTE
SwitchG	fa0/1	CoreSwitchC	fa0/13	XO
	fa0/2	RouterG	fa0/0	ST
	fa0/11	CoreSwitchA	fa0/7	XO
	fa0/12	CoreSwitchB	fa0/7	XO
RouterH	fa0/0	SwitchH	fa0/2	ST
	fa0/1	CoreSwitchC	fa0/16	ST
	s0/0/0	CoreRouter	s1/7	DTE
	s0/1	RouterG	s0/1	DCE
SwitchH	fa0/1	CoreSwitchC	fa0/15	XO
	fa0/2	RouterH	fa0/0	ST
	fa0/11	CoreSwitchA	fa0/8	XO
	fa0/12	CoreSwitchB	fa0/8	XO

Note ST = straight RJ-45, XO = crossover RJ-45

Table 5: CoreSwitchA Cabling

VLAN	Interface	Remote Device	Interface	Remarks
11	fa0/1	SwitchA	fa0/11	XO
12	fa0/2	SwitchB	fa0/11	XO
13	fa0/3	SwitchC	fa0/11	XO
14	fa0/4	SwitchD	fa0/11	XO
15	fa0/5	SwitchE	fa0/11	XO
16	fa0/6	SwitchF	fa0/11	XO
17	fa0/7	SwitchG	fa0/11	XO
18	fa0/8	SwitchH	fa0/11	XO
-	fa0/9-fa0/12	Unused	Unused	Unused
Trunk	fa0/13	CoreSwitchB	fa0/13	XO-
Shutdown	fa0/14	CoreSwitchB	fa0/14	XO-
-	fa0/15-fa0/21	Unused	Unused	Unused
Trunk	fa0/22	CoreSwitchC	fa0/22	XO
Trunk	fa0/23	CoreRouter	fa0/0	ST
Trunk	fa0/24	TFTP		ST
-	gi0/1	Unused	Unused	Unused
-	gi0/2	Unused	Unused	Unused

Table 6: CoreSwitchB Cabling

VLAN	Interface	Remote Device	Interface	Remarks
51	fa0/1	SwitchA	fa0/12	XO
52	fa0/2	SwitchB	fa0/12	XO
53	fa0/3	SwitchC	fa0/12	XO
54	fa0/4	SwitchD	fa0/12	XO
55	fa0/5	SwitchE	fa0/12	XO
56	fa0/6	SwitchF	fa0/12	XO
57	fa0/7	SwitchG	fa0/12	XO
58	fa0/8	SwitchH	fa0/12	XO
-	fa0/9-fa0/12	Unused	Unused	Unused
Trunk	fa0/13	CoreSwitchA	fa0/13	XO
Shutdown	fa0/14	CoreSwitchA	fa0/14	XO
-	fa0/15-fa0/24	Unused	Unused	Unused
-	gi0/1	Unused	Unused	Unused
-	gi0/2	Unused	Unused	Unused

Note VTP domain = icnd1

Table 7: CoreSwitchC Cabling

VLAN	Interface	Remote Device	Interface	Remarks
31/61	fa0/1	SwitchA	fa0/1	XO
41	fa0/2	RouterA	fa0/1	ST
32/62	fa0/3	SwitchB	fa0/1	XO
42	fa0/4	RouterB	fa0/1	ST
33/63	fa0/5	SwitchC	fa0/1	XO
43	fa0/6	RouterC	fa0/1	ST
34/64	fa0/7	SwitchD	fa0/1	XO
44	fa0/8	RouterD	fa0/1	ST
35/65	fa0/9	SwitchE	fa0/1	XO
45	fa0/10	RouterE	fa0/1	ST
36/66	fa0/11	SwitchF	fa0/1	XO
46	fa0/12	RouterF	fa0/1	ST
37/67	fa0/13	SwitchG	fa0/1	XO
47	fa0/14	RouterG	fa0/1	ST
38/68	fa0/15	SwitchH	fa0/1	XO
48	fa0/16	RouterH	fa0/1	ST
-	fa0/17-fa0/21	Unused	Unused	Unused
Trunk	fa0/22	CoreSwitchA	fa0/22	XO
-	fa0/23	Unused	Unused	Unused
Trunk	fa0/24	CoreRouter	fa0/1	ST
Trunk	gi0/1	VPN/TS	fa0/1	ST
-	gi0/2	Unused	Unused	Unused

Note VLAN 3*x* is used for *all* labs except Lab 6-4, in which VLAN 6*x* is used.

Table 8: VPN/TS Cabling

VLAN	Interface	Remote Device	Interface	IP / Remarks
-	fa0/0	ISP access	??	To ISP
1	fa0/1.1	CoreSwitchC	gi0/1	10.1.1.100
31	fa0/1.31	CoreSwitchC	gi0/1	10.2.2.100
32	fa0/1.32	CoreSwitchC	gi0/1	10.3.3.100
33	fa0/1.33	CoreSwitchC	gi0/1	10.4.4.100
34	fa0/1.34	CoreSwitchC	gi0/1	10.5.5.100
35	fa0/1.35	CoreSwitchC	gi0/1	10.6.6.100
36	fa0/1.36	CoreSwitchC	gi0/1	10.7.7.100
37	fa0/1.37	CoreSwitchC	gi0/1	10.8.8.100
38	fa0/1.38	CoreSwitchC	gi0/1	10.9.9.100
61	fa0/1.61	CoreSwitchC	gi0/1	10.22.22.100
62	fa0/1.62	CoreSwitchC	gi0/1	10.33.33.100
63	fa0/1.63	CoreSwitchC	gi0/1	10.44.44.100
64	fa0/1.64	CoreSwitchC	gi0/1	10.55.55.100
65	fa0/1.65	CoreSwitchC	gi0/1	10.66.66.100
66	fa0/1.66	CoreSwitchC	gi0/1	10.77.77100
67	fa0/1.67	CoreSwitchC	gi0/1	10.88.88.100
68	fa0/1.68	CoreSwitchC	gi0/1	10.99.99.100
99	fa0/1.99	CoreSwitchC	gi0/1	Trunk VLAN

Table 9: VPN/TS Console Cabling

Hardware	TTY	Line	Remote Device	Type	Cable ID
NM 1	66	Line 1/0	RouterA	Console	Octal cable 1/1
NM 1	67	Line 1/1	SwitchA	Console	Octal cable 1/2
NM 1	68	Line 1/2	RouterB	Console	Octal cable 1/3
NM 1	69	Line 1/3	SwitchB	Console	Octal cable 1/4
NM 1	70	Line 1/4	RouterC	Console	Octal cable 1/5
NM 1	71	Line 1/5	SwitchC	Console	Octal cable 1/6
NM 1	72	Line 1/6	RouterD	Console	Octal cable 1/7
NM 1	73	Line 1/7	SwitchD	Console	Octal cable 1/8
NM 1	74	Line 1/8	CoreSwitchA	Console	Octal cable 2/1
NM 1	75	Line 1/9	CoreSwitchB	Console	Octal cable 2/2
NM 1	76	Line 1/10	CoreSwitchC	Console	Octal cable 2/3
NM 1	77	Line 1/11	CoreRouter	Console	Octal cable 2/4
NM 1	78	Line 1/12	Spare	Console	Octal cable 2/5
NM 1	79	Line 1/13	APC1	Console	Octal cable 2/6
NM 1	80	Line 1/14	APC2	Console	Octal cable 2/7
NM 1	81	Line 1/15	APC3	Console	Octal cable 2/8
HWIC0/0/0	2	Line 0/0/0	RouterE	Console	HD Octal cable P0
HWIC0/0/0	3	Line 0/0/1	SwitchE	Console	HD Octal cable P1
HWIC0/0/0	4	Line 0/0/2	RouterF	Console	HD Octal cable P2
HWIC0/0/0	5	Line 0/0/3	SwitchF	Console	HD Octal cable P3
HWIC0/0/0	6	Line 0/0/3	RouterG	Console	HD Octal cable P4
HWIC0/0/0	7	Line 0/0/5	SwitchG	Console	HD Octal cable P5
HWIC0/0/0	8	Line 0/0/6	RouterH	Console	HD Octal cable P6
HWIC0/0/0	9	Line 0/0/7	SwitchH	Console	HD Octal cable P7

Table 10: CoreRouter Cabling—Physical Interfaces

CoreRouter	Interface	Remote Device	Interface	Remarks
	s1/0	RouterA	s0/0/0	DCE
	s1/1	RouterB	s0/0/0	DCE
	s1/2	RouterC	s0/0/0	DCE
	s1/3	RouterD	s0/0/0	DCE
	s1/4	RouterE	s0/0/0	DCE
	s1/5	RouterF	s0/0/0	DCE
	s1/6	RouterG	s0/0/0	DCE
	s1/7	RouterH	s0/0/0	DCE
	s0/0/0	CoreRouter	s0/0/1	Loop-Back DCE
	s0/0/1	CoreRouter	s0/0/0	Loop-Back DTE
	fa0/0	CoreSwitchB	gi1/2	Trunk RJ-45
	fa0/1	CoreSwitchC	fa0/24	Trunk RJ-45

Table 11: APC1 Power Cable Connections

Device	Power Outlet	Device		Remarks
APC1	1	RouterA		Power Cord
	2	SwitchA		Power Cord
	3	RouterB		Power Cord
	4	SwitchB		Power Cord
	5	RouterC		Power Cord
	6	SwitchC		Power Cord
	7	RouterD		Power Cord
	8	SwitchD		Power Cord

Table 12: APC2 Power Cable Connections

Device	Power Outlet	Device		Remarks
APC2	1	RouterE		Power Cord
	2	SwitchE		Power Cord
	3	RouterF		Power Cord
	4	SwitchF		Power Cord
	5	RouterG		Power Cord
	6	SwitchG		Power Cord
	7	RouterH		Power Cord
	8	SwitchH		Power Cord

Table 13: APC3 Power Cable Connections

Device	Power Outlet	Device		Remarks
APC3	1	CoreSwitchA		Power Cord
	2	CoreSwitchB		Power Cord
	3	CoreSwitchC		Power Cord
	4	CoreRouter		Power Cord
	5	Spare		Unused
	6	Spare		Unused
	7	Spare		Unused
	8	Spare		Unused

A TFTP server is required and needs to support a 802.1Q Ethernet adapter with nine VLANs total.

Table 14: TFTP Server VLAN

VLAN	Primary IP Address /24	Secondary IP Address /24
1	10.1.1.1	none
51	10.2.2.1	10.22.22.1
52	10.3.3.1	10.33.33.1
53	10.4.4.1	10.44.44.1
54	10.5.5.1	10.55.55.1
55	10.6.6.1	10.66.66.1
56	10.7.7.1	10.77.77.1
57	10.8.8.1	10.88.88.1
58	10.9.9.1	10.99.99.1

General Lab Setup

This information details the procedure to set up and configure the lab equipment at the beginning of each class.

Step 1 Download the initial core configuration from the TFTP server into the startup-configuration of each of the core devices. The initial core configuration files:

Device	Configuration File to Install
CoreRouter	i1-corero-startup.txt
CoreSwitchA	i1-coreswa-all.txt
CoreSwitchB	i1-coreswb-all.txt
CoreSwitchC	i1-coreswc-startup.txt
VPNTS	vpnts-all.txt
Workgroup Switches	None
Workgroup Routers	flash:sdmconfig-2811.cfg
TFTP server	descript-config
TFTP server	c2800nm-advipservicesk9-mz.124-12.bin

Learners will create their own workgroup configurations as labs proceed.

Step 2 Reload each core device.

Lab 1-1: Using Windows Applications as Network Tools

This topic details the lab activity for Lab 1-1.

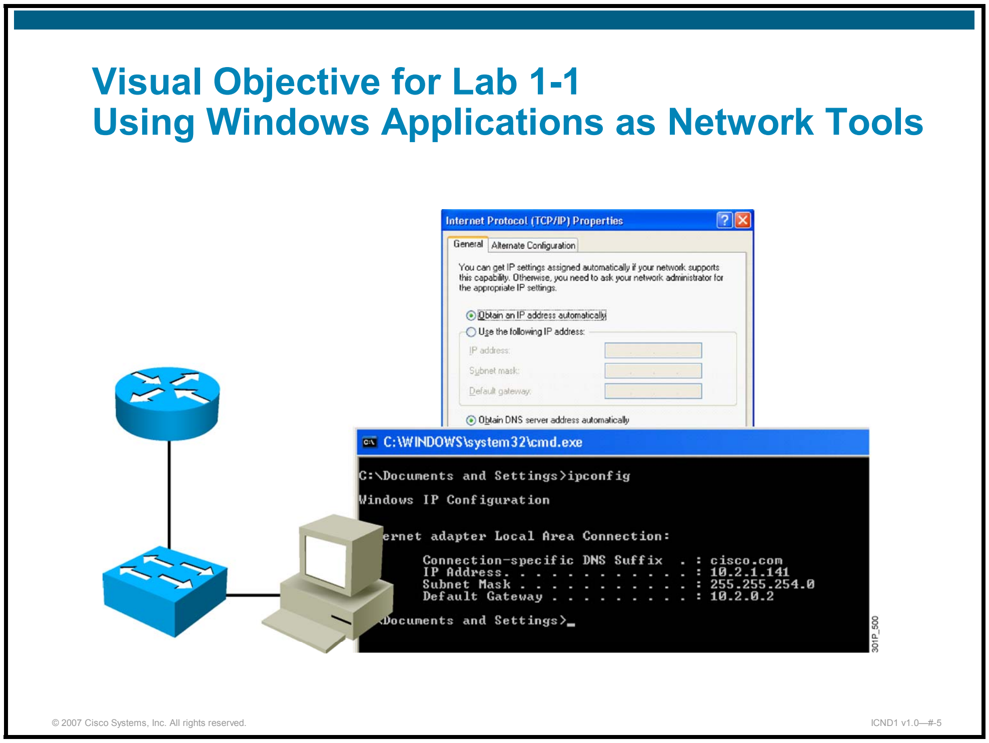
Objectives

You will complete these tasks in this lab:

- Using the windows command **ipconfig**, be able to determine PC current network addressing information.
- Using the windows command **ping**, be able to determine test connectivity to the default gateway router.
- Using the windows command **arp –a**, be able to view the local PC ARP table and determine the association between the IP address and the MAC address of the default gateway.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 1-1
Using Windows Applications as Network Tools

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:
● Obtain DNS server address automatically

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

ernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cisco.com
        IP Address. . . . . . . . . . . . : 10.2.1.141
        Subnet Mask . . . . . . . . . . . : 255.255.254.0
        Default Gateway . . . . . . . . . : 10.2.0.2

 Documents and Settings>_
```

Setup

The lab requires a Windows PC with access to the local network.

Additional Setup Notes

Desktop icons for the following applications:

- Windows Command window
- Shortcut to the properties of the Ethernet adapter used to access the network

Common Issues

There are no known issues.

Lab 1-2: Observing the TCP Three-Way Handshake

This topic details the lab activity for Lab 1-2.

Objectives

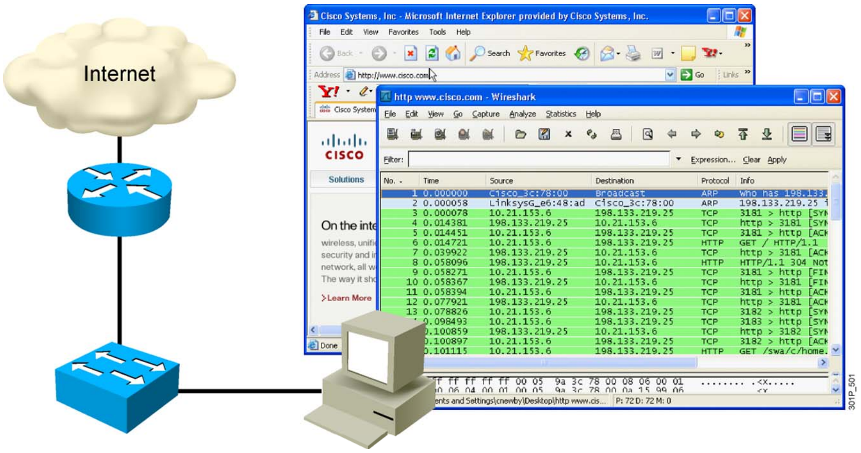
You will complete these tasks in this lab:

- Start the packet sniffer software application to monitor the appropriate Ethernet interface for recording the packet flow.
- Generate a TCP connection using a web browser.
- Observe the initial packets of the TCP flow, especially the SYN packet, SYN ACK packet, and finally the ACK packet.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.

Visual Objective for Lab 1-2
Observing the TCP Three-Way Handshake


Internet
Cisco Systems, Inc - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
http://www.cisco.com
http www.cisco.com - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
301P_501

```
No. -  Time      Source             Destination        Protocol Info
  1 0.000000  Cisco_3c:78:00     Broadcast          ARP      Who has 198.133.
  2 0.000058  LinksysG_e6:48:ad  Cisco_3c:78:00     ARP      198.133.219.25 i
  3 0.000078  10.21.153.6        198.133.219.25     TCP      3181 > http [SYN
  4 0.014381  198.133.219.25     10.21.153.6        TCP      http > 3181 [SYN
  5 0.014451  10.21.153.6        198.133.219.25     TCP      3181 > http [ACK
  6 0.014721  10.21.153.6        198.133.219.25     HTTP     GET / HTTP/1.1
  7 0.039922  198.133.219.25     10.21.153.6        TCP      http > 3181 [ACK
  8 0.058096  198.133.219.25     10.21.153.6        HTTP     HTTP/1.1 304 Not
  9 0.058271  10.21.153.6        198.133.219.25     TCP      3181 > http [FIN
 10 0.058367  198.133.219.25     10.21.153.6        TCP      http > 3181 [FIN
 11 0.058394  10.21.153.6        198.133.219.25     TCP      3181 > http [ACK
 12 0.077921  198.133.219.25     10.21.153.6        TCP      http > 3181 [ACK
 13 0.078826  10.21.153.6        198.133.219.25     TCP      3182 > http [SYN
    0.098493  10.21.153.6        198.133.219.25     TCP      3183 > http [SYN
    0.100859  198.133.219.25     10.21.153.6        TCP      http > 3182 [SYN
    0.100897  10.21.153.6        198.133.219.25     TCP      3182 > http [ACK
    0.101115  10.21.153.6        198.133.219.25     HTTP     GET /swa/c/home.

ff ff ff ff ff 00 05   9a 3c 78 00 08 06 00 01   ........ .<X.....
0 06 04 00 01 00 05   9a 3c 78 00 0a 15 99 06
ents and Settings\cnewby\Desktop\http www.cis...   P: 72 D: 72 M: 0
```

© 2007 Cisco Systems, Inc. All rights reserved.   ICND1 v1.0—#-6

Setup

No special setup required.

Additional Setup Notes

Desktop icons for the following applications:

- Wireshark
- Windows Explorer

Instructor Notes

The learners are strongly cautioned that using a packet sniffer in their work environment may be a breach of their employers' security policy, and it is worthwhile to reinforce that statement prior to the start of the lab.

Common Issues

This subtopic presents common issues for this lab.

- Depending on how busy the local network is, this will depend on how easy learners are able to find the TCP sequence in the captured packets window.
- Use of the preconfigured Wireshark TCP filter.

Lab 1-3: Observing Extended PC Network Information

This topic details the lab activity for Lab 1-3.

Objectives

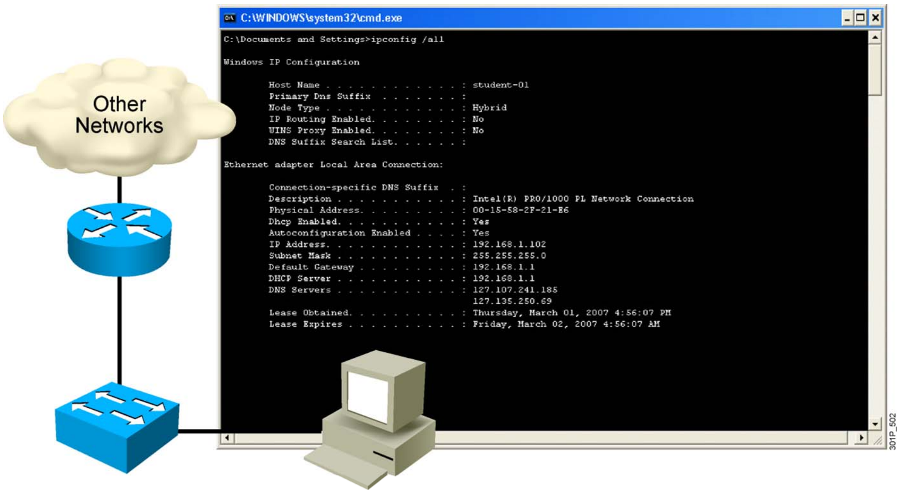
You will complete these tasks in this lab:

- Using the windows command **ipconfig /all**, be able to determine IP addresses of the DNS servers available to your PC.
- Using the IP address of one of the DNS servers from Task 1, test connectivity to the DNS servers using the windows **ping** command.
- Using the windows command **tracert /d**, obtain the IP addresses of the routers traversed to reach the DNS server tested in Task 2.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.

Visual Objective for Lab 1-3
Observing Extended PC Network Information



```
C:\Documents and Settings>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : student-01
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . :

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/1000 PL Network Connection
        Physical Address. . . . . . . . . : 00-15-58-2F-21-E6
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.102
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 127.107.241.185
                                            127.135.250.69
        Lease Obtained. . . . . . . . . . : Thursday, March 01, 2007 4:56:07 PM
        Lease Expires . . . . . . . . . . : Friday, March 02, 2007 4:56:07 AM
```

ICND1 v1.0—#-7

Setup

Same as for previous lab.

Instructor Notes

The DNS server was chosen as the target of the ping and trace as a demonstration of using information gathered from the **ipconfig** command. You could also get the learners to use the following: www.example.com, www.example.org.

Common Issues

There are no known issues.

Lab 2-1: Connecting to Remote Lab Equipment

This topic details the lab activity for Lab 2-1.

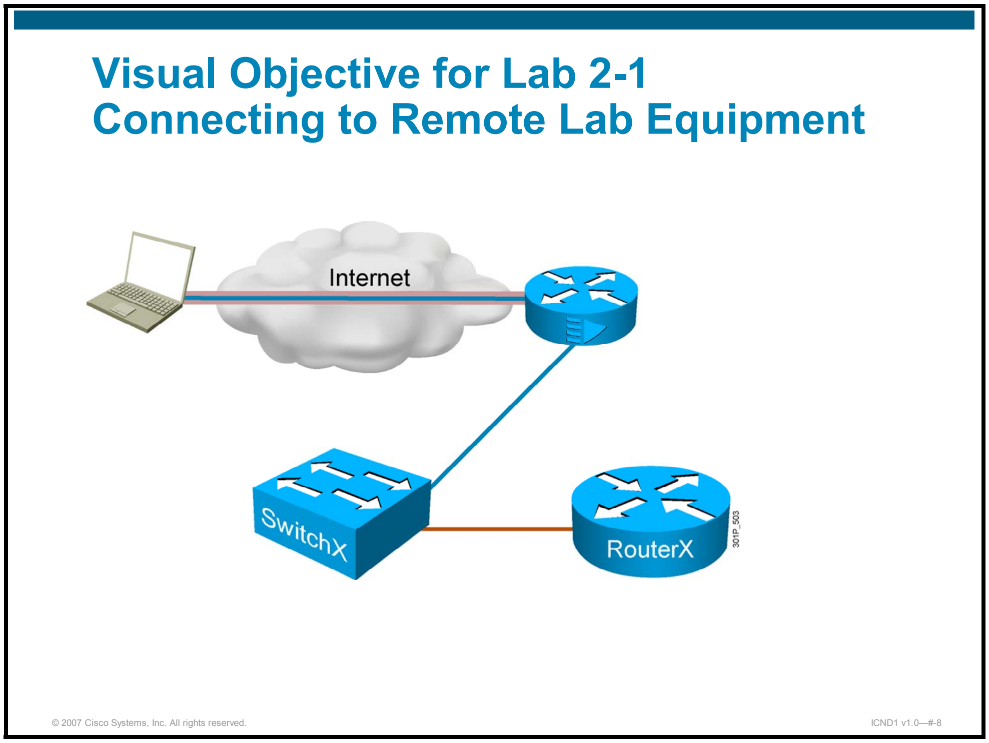
Objectives

You will complete these tasks in this lab:

- Connect to your assigned workgroup equipment using a console (terminal) server, so that switches and routers can be configured via the console ports.
- Connect to your assigned workgroup equipment using the VPN client software, so that your PC is connected through an interface on your workgroup switch. This will allow the configuration of your workgroup router using Cisco SDM.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-1
Connecting to Remote Lab Equipment

ICND1 v1.0—#-8

Setup

Desktop icons for the following applications:

- PuTTY
- Cisco VPN Client
- Cisco VPN Client profiles from CD loaded in profiles folder.

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	This file should be in the startup-config
CoreSwitchA	i1-coreswa-all.txt	This file should be in the startup-config
CoreSwitchB	i1-coreswb-all.txt	This file should be in the startup-config
CoreSwitchC	i1-coreswc-startup.txt	This file should be in the startup-config
VPNTS	vpnts-all.txt	This file should be in the startup-config
WG switches	none	
WG routers	sdm-2811.cfg	This file should be in the startup-config

Instructor Notes

This lab gives the learner the opportunity to practice connecting to the remote lab. You should have the information necessary for the learners to complete Table 1 of the lab.

Table 1 Network and Connection Information

Information	Instructor-Assigned Value
Your assigned workgroup (letter)	
IP address of the *console server*	
Username and password for SSH	
IP address of the *VPN-RTR (if different from above)*	
VPN Client connection entry name	
Username and password for VPN (if different from SSH)	
SSH terminal emulation application	

Highlight the reason for having two connection methods.

- SSH connects over the Internet to the console server, which in turn allows them to access the console ports of their assigned switch and router via a menu front end.
- VPN tunnel connects through the Internet and allows the PC in the classroom to directly address their workgroup switch and router, allowing use of GUI management tools such as Cisco SDM.

You could take the opportunity to explain how each workgroup is considered a separate entity and does *not* interact with other workgroups. The object of the class and labs is to give the learners a complete set of skills so that, under supervision, they can configure and test a small branch network.

Common Issues

There are no known issues.

Lab 2-2: Performing Switch Startup and Initial Configuration

This topic details the lab activity for Lab 2-2.

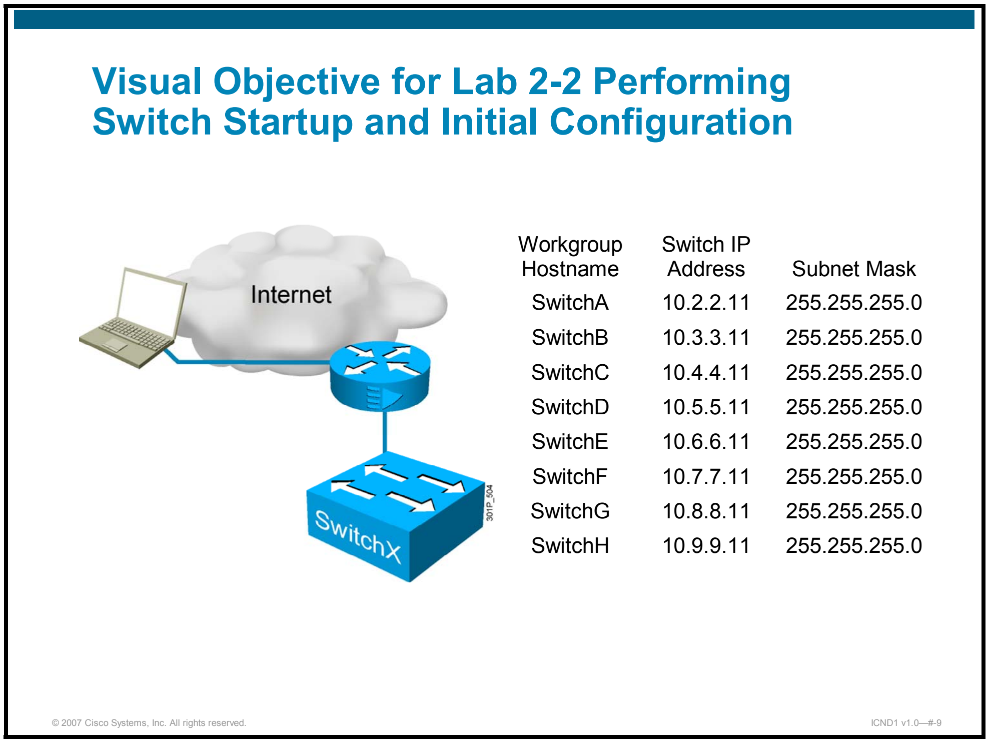
Objectives

You will complete these tasks in this lab:

- Restart the switch and verify the initial configuration messages.
- Complete the initial configuration of the Cisco Catalyst switch.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-2 Performing Switch Startup and Initial Configuration

Workgroup Hostname	Switch IP Address	Subnet Mask
SwitchA	10.2.2.11	255.255.255.0
SwitchB	10.3.3.11	255.255.255.0
SwitchC	10.4.4.11	255.255.255.0
SwitchD	10.5.5.11	255.255.255.0
SwitchE	10.6.6.11	255.255.255.0
SwitchF	10.7.7.11	255.255.255.0
SwitchG	10.8.8.11	255.255.255.0
SwitchH	10.9.9.11	255.255.255.0

ICND1 v1.0—#-9

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab
WG switches	none	same as previous lab
WG routers	sdm-2811.cfg	same as previous lab

Instructor Notes

If you have not done so before, you need to assign the learners to their workgroups.

Draw the learner's attention to the job aid tables at the beginning of the lab. Explain that there are answers in the back of the Lab Guide giving the ending configuration for each lab. If the lab does *not* change a configuration, the assumption is that the prior configuration should be referenced.

Common Issues

There are no known issues.

Lab 2-3: Enhancing the Security of Initial Switch Configuration

This topic details the lab activity for Lab 2-3.

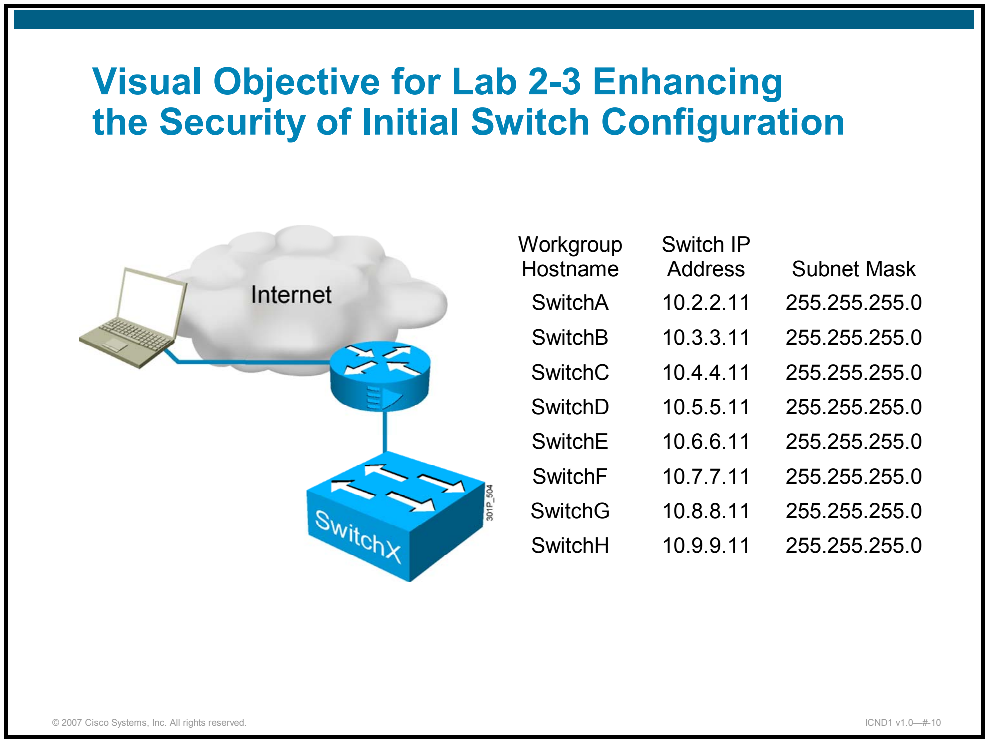
Objectives

You will complete these tasks in this lab:

- Add password protection to the console and vty lines.
- Use the Cisco IOS configuration command to encrypt all passwords.
- Add a banner message to the login process.
- Increase the security of remote management of the switch by adding SSH protocol to the virtual terminal lines.
- Increase the security of the physical interfaces by configuring various methods of MAC address security.
- Disable unused interfaces.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-3 Enhancing the Security of Initial Switch Configuration

Workgroup Hostname	Switch IP Address	Subnet Mask
SwitchA	10.2.2.11	255.255.255.0
SwitchB	10.3.3.11	255.255.255.0
SwitchC	10.4.4.11	255.255.255.0
SwitchD	10.5.5.11	255.255.255.0
SwitchE	10.6.6.11	255.255.255.0
SwitchF	10.7.7.11	255.255.255.0
SwitchG	10.8.8.11	255.255.255.0
SwitchH	10.9.9.11	255.255.255.0

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-10

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This is one of the longer labs. The emphasis is on increasing the security of the network and the switch. Not all aspects of security are covered here; for example, Cisco Discovery Protocol is covered later.

Common Issues

There are no known issues.

Lab 2-4: Operating and Configuring a Cisco IOS Device

This topic details the lab activity for Lab 2-4.

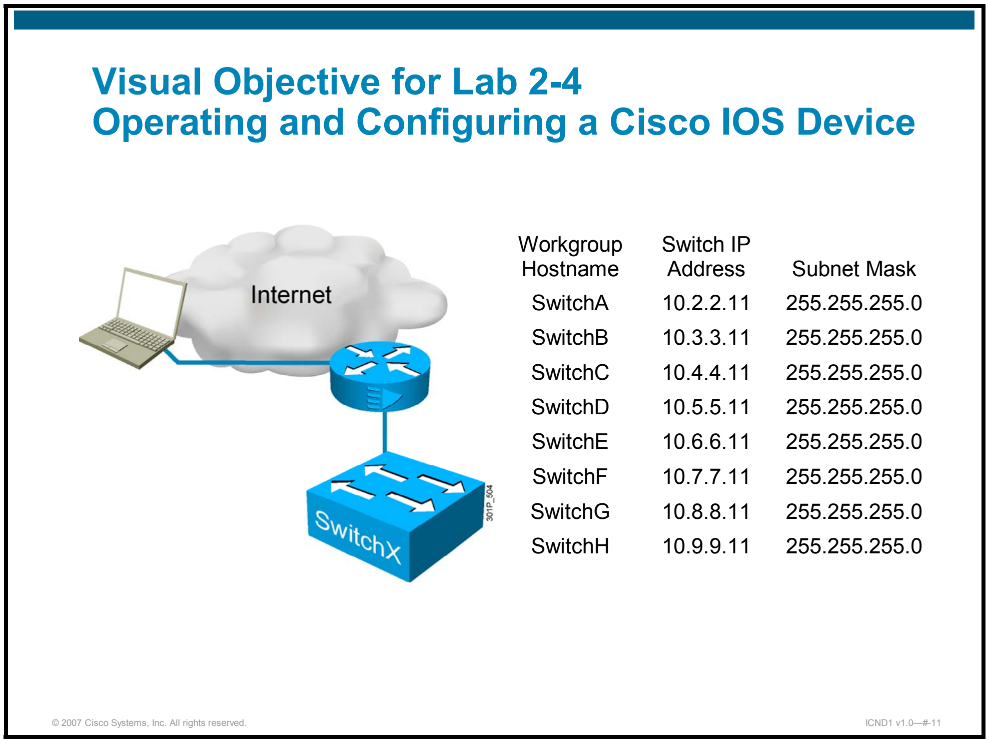
Objectives

You will complete these tasks in this lab:

- Explore context-sensitive help.
- Edit incorrect CLI commands on the switch.
- Examine the switch status using **show** commands.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 2-4
Operating and Configuring a Cisco IOS Device

Workgroup Hostname	Switch IP Address	Subnet Mask
SwitchA	10.2.2.11	255.255.255.0
SwitchB	10.3.3.11	255.255.255.0
SwitchC	10.4.4.11	255.255.255.0
SwitchD	10.5.5.11	255.255.255.0
SwitchE	10.6.6.11	255.255.255.0
SwitchF	10.7.7.11	255.255.255.0
SwitchG	10.8.8.11	255.255.255.0
SwitchH	10.9.9.11	255.255.255.0

ICND1 v1.0—#-11

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab provides practice using the CLI and also tailoring it to be more user-friendly.

Although most terminal emulation programs allow the use of the arrow keys to move up, down, forward, and backward, the Ctrl keys are still useful. **Ctrl-A** and **Ctrl-E** accelerate the movement within the CLI.

Common Issues

There are no known issues.

Lab 4-1: Converting Decimal to Binary and Binary to Decimal

This topic details the lab activity for Lab 4-1.

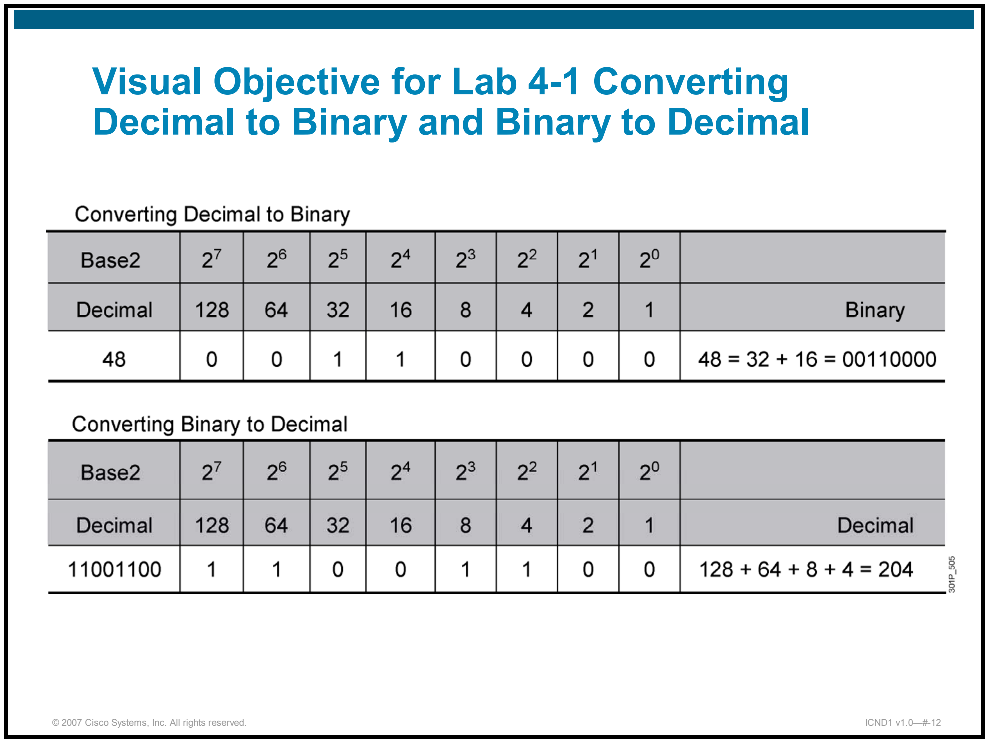
Objectives

You will complete these tasks in this lab:

- Convert decimal numbers to binary numbers.
- Convert binary numbers to decimal numbers.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-1 Converting Decimal to Binary and Binary to Decimal

Converting Decimal to Binary

Base2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Decimal	128	64	32	16	8	4	2	1	Binary
48	0	0	1	1	0	0	0	0	48 = 32 + 16 = 00110000

Converting Binary to Decimal

Base2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Decimal	128	64	32	16	8	4	2	1	Decimal
11001100	1	1	0	0	1	1	0	0	128 + 64 + 8 + 4 = 204

301P_505

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-12

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab is essentially practicing the skills of the lesson. The remote lab is not used during this lab.

Common Issues

There are no known issues.

Lab 4-2: Classifying Network Addressing

This topic details the lab activity for Lab 4-2.

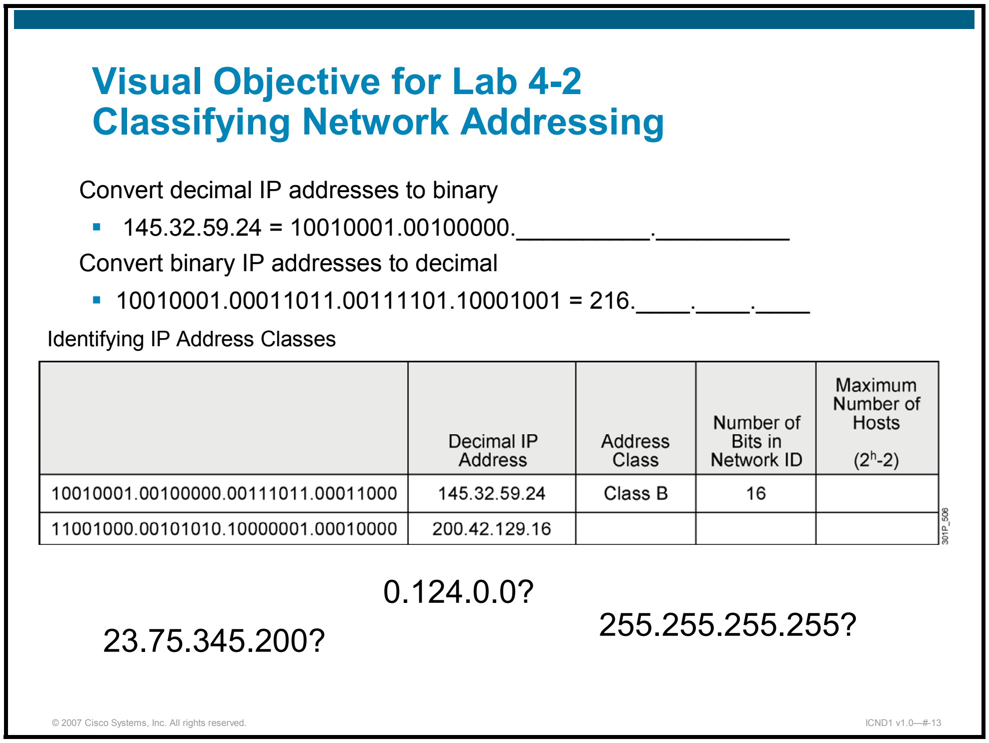
Objectives

You will complete these tasks in this lab:

- Convert decimal IP addresses to binary numbers.
- Convert binary numbers to IP addresses.
- Identify classes of IP addresses.
- Identify valid and invalid host IP addresses.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-2 Classifying Network Addressing

Convert decimal IP addresses to binary

- 145.32.59.24 = 10010001.00100000.__________.__________

Convert binary IP addresses to decimal

- 10010001.00011011.00111101.10001001 = 216.____.____.____

Identifying IP Address Classes

	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2^h-2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	
11001000.00101010.10000001.00010000	200.42.129.16			

0.124.0.0?

23.75.345.200?

255.255.255.255?

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab is essentially practicing the skills of the lesson. The remote lab is not used during this lab.

Common Issues

There are no known issues.

Lab 4-3: Computing Usable Subnetworks and Hosts

This topic details the lab activity for Lab 4-3.

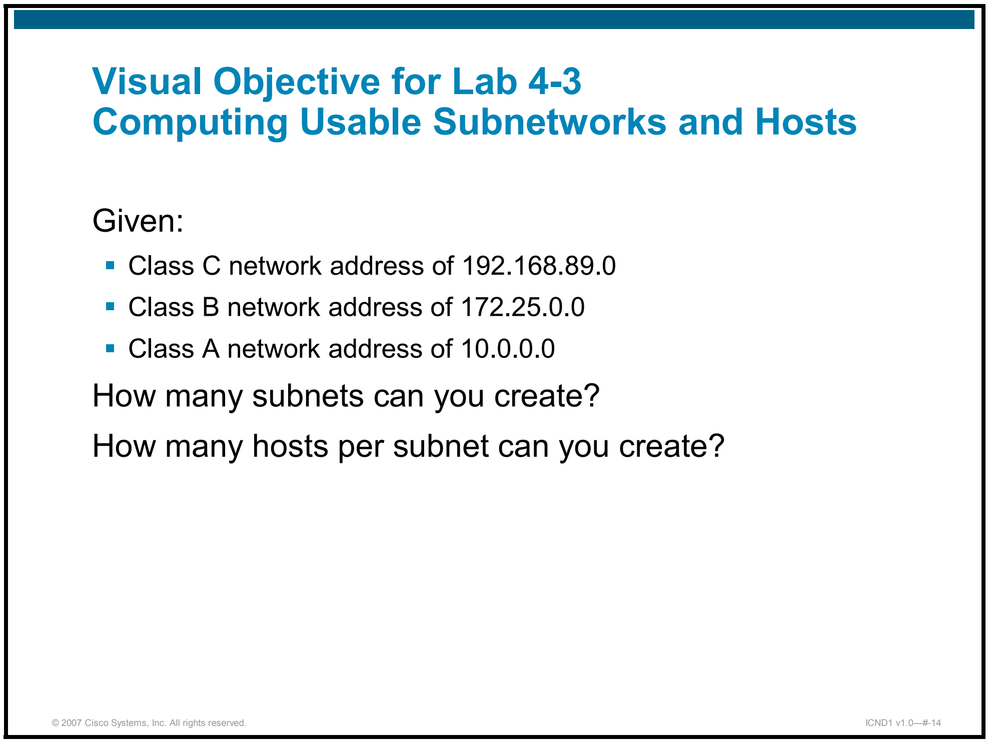
Objectives

You will complete these tasks in this lab:

- Determine the number of bits required to create different subnets.
- Determine the maximum number of host addresses available in a given subnet.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-3 Computing Usable Subnetworks and Hosts

Given:

- Class C network address of 192.168.89.0
- Class B network address of 172.25.0.0
- Class A network address of 10.0.0.0

How many subnets can you create?

How many hosts per subnet can you create?

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-14

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab is essentially practicing the skills of the lesson. The remote lab is not used during this lab.

Common Issues

There are no known issues.

Lab 4-4: Calculating Subnet Masks

This topic details the lab activity for Lab 4-4.

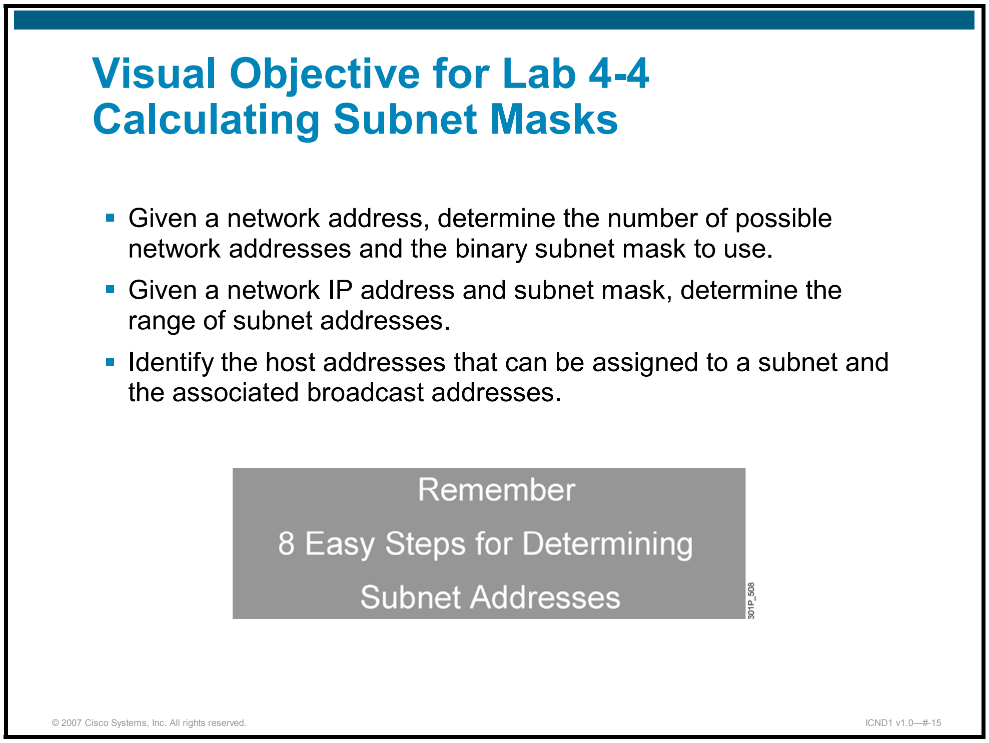
Objectives

You will complete these tasks in this lab:

- Given a network address, determine the number of possible network addresses and the binary subnet mask to use.
- Given a network IP address and subnet mask, determine the range of subnet addresses.
- Identify the host addresses that can be assigned to a subnet and the associated broadcast addresses.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-4
Calculating Subnet Masks

- Given a network address, determine the number of possible network addresses and the binary subnet mask to use.
- Given a network IP address and subnet mask, determine the range of subnet addresses.
- Identify the host addresses that can be assigned to a subnet and the associated broadcast addresses.

Remember

8 Easy Steps for Determining

Subnet Addresses

301P_508

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-15

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab is essentially practicing the skills of the lesson. The remote lab is not used during this lab.

Common Issues

There are no known issues.

Lab 4-5: Performing Initial Router Startup

This topic details the lab activity for Lab 4-5.

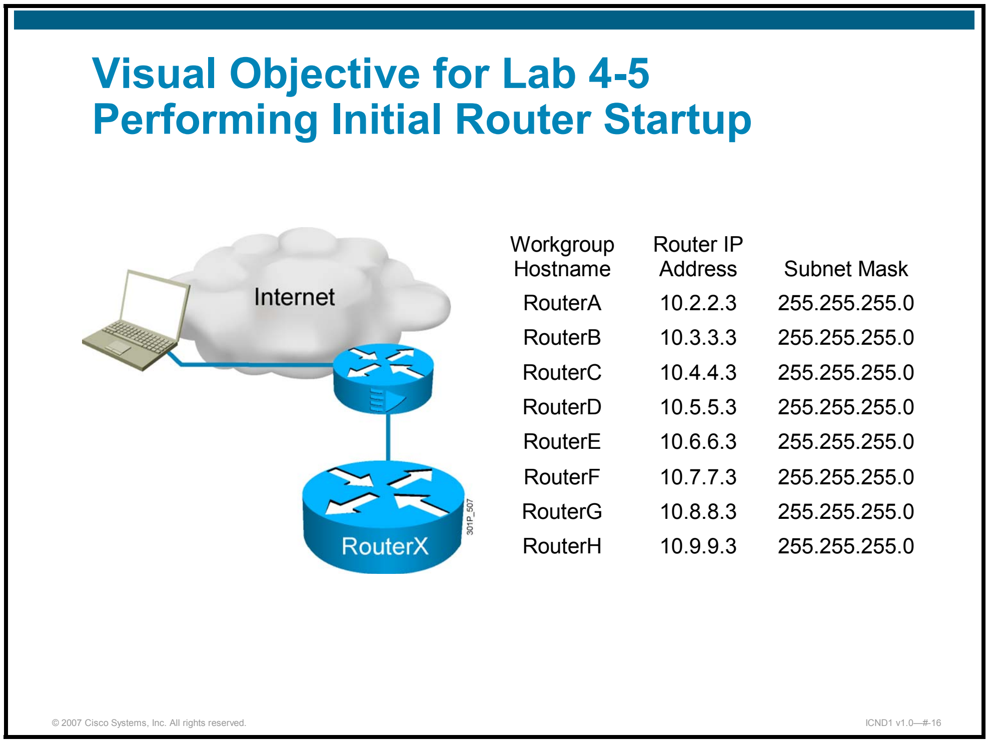
Objectives

You will complete these tasks in this lab:

- Remove any existing residual router configuration.
- Restart the router and observe the output.
- Decline the Initial Configuration Dialog request when the restart process completes.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-5
Performing Initial Router Startup

Workgroup Hostname	Router IP Address	Subnet Mask
RouterA	10.2.2.3	255.255.255.0
RouterB	10.3.3.3	255.255.255.0
RouterC	10.4.4.3	255.255.255.0
RouterD	10.5.5.3	255.255.255.0
RouterE	10.6.6.3	255.255.255.0
RouterF	10.7.7.3	255.255.255.0
RouterG	10.8.8.3	255.255.255.0
RouterH	10.9.9.3	255.255.255.0

ICND1 v1.0—#-16

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

Although this lab assumes that the router has a Cisco SDM configuration in startup, it is written to work with unconfigured NVRAM also. Unlike the switch configuration lab, the learners decline using configuration dialog directly.

Common Issues

This subtopic presents a common issue for this lab.

- **Task 2, Step 3, Output:** The output shows “sslinit fn.” This is not an error or mistype. The output can be interpreted as the SSL protocol function in the encryption logic initializing.

Lab 4-6: Performing Initial Router Configuration

This topic details the lab activity for Lab 4-6.

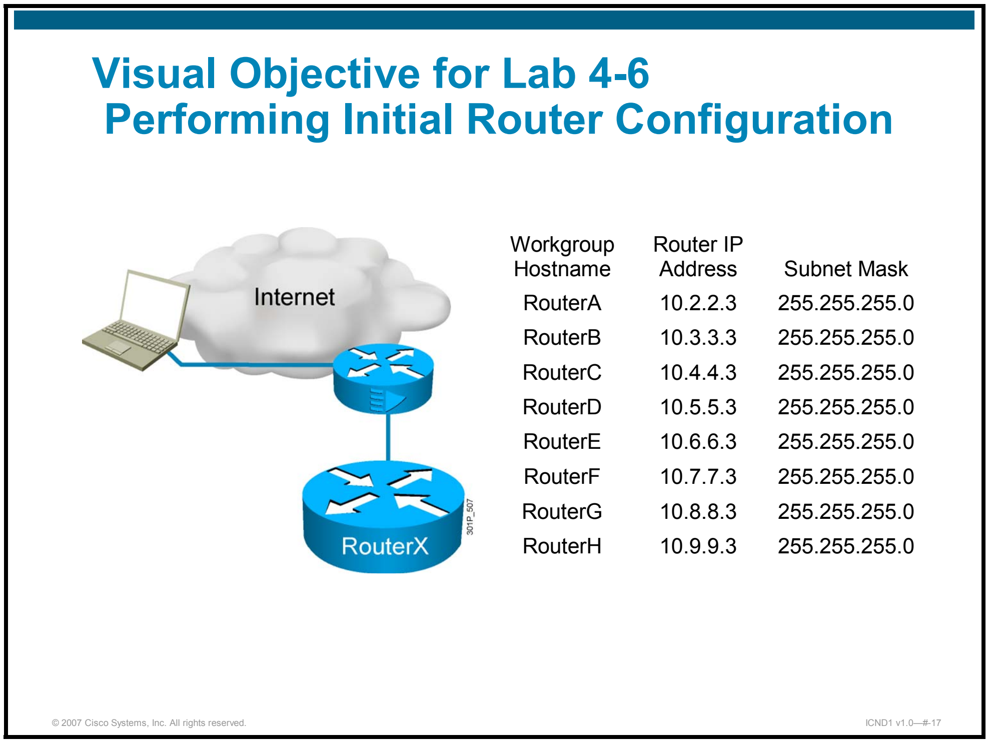
Objectives

You will complete these tasks in this lab:

- Use the **setup** command to apply a minimal configuration for router operation.
- Use the **show** commands to validate your configuration.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-6
Performing Initial Router Configuration

Workgroup Hostname	Router IP Address	Subnet Mask
RouterA	10.2.2.3	255.255.255.0
RouterB	10.3.3.3	255.255.255.0
RouterC	10.4.4.3	255.255.255.0
RouterD	10.5.5.3	255.255.255.0
RouterE	10.6.6.3	255.255.255.0
RouterF	10.7.7.3	255.255.255.0
RouterG	10.8.8.3	255.255.255.0
RouterH	10.9.9.3	255.255.255.0

ICND1 v1.0—#-17

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

The learners will use the **setup** command to enter an initial configuration on their workgroup router.

Common Issues

There are no known issues.

Lab 4-7: Enhancing the Security of the Initial Router Configuration

This topic details the lab activity for Lab 4-7.

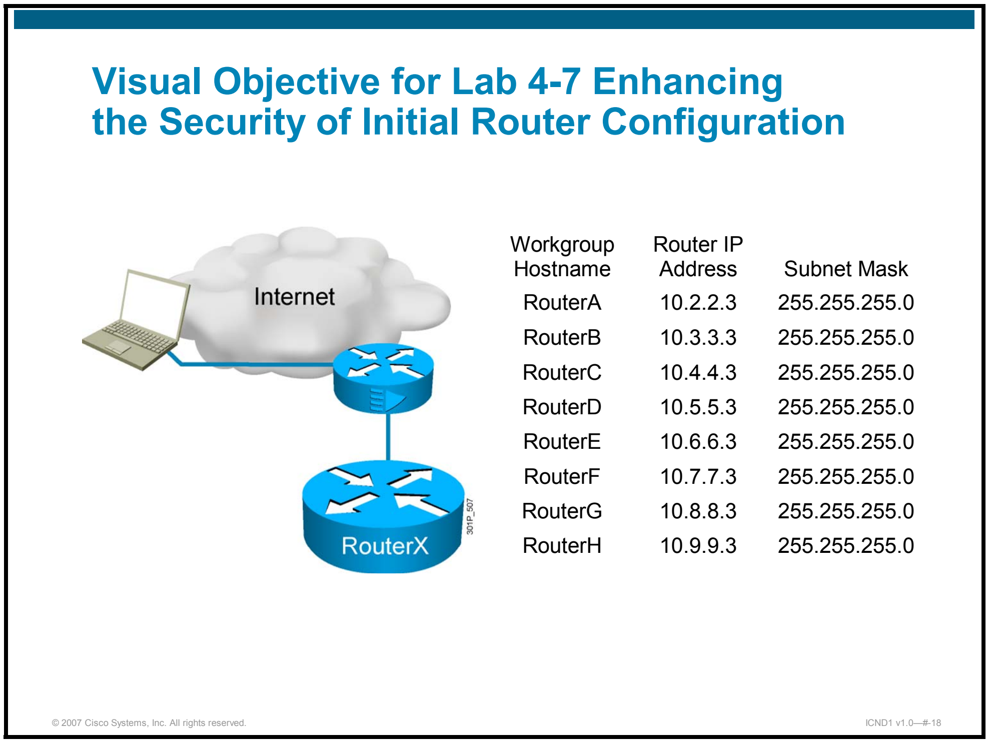
Objectives

You will complete these tasks in this lab:

- Add password protection to the console line.
- Use the Cisco IOS configuration command to encrypt all passwords.
- Add a banner message to the login process.
- Increase the remote management security of the router by adding SSH protocol to the virtual terminal lines.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-7 Enhancing the Security of Initial Router Configuration

Workgroup Hostname	Router IP Address	Subnet Mask
RouterA	10.2.2.3	255.255.255.0
RouterB	10.3.3.3	255.255.255.0
RouterC	10.4.4.3	255.255.255.0
RouterD	10.5.5.3	255.255.255.0
RouterE	10.6.6.3	255.255.255.0
RouterF	10.7.7.3	255.255.255.0
RouterG	10.8.8.3	255.255.255.0
RouterH	10.9.9.3	255.255.255.0

ICND1 v1.0—#-18

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab adds security and CLI usability enhancements to the basic configuration.

Common Issues

There are no known issues.

Lab 4-8: Using Cisco SDM to Configure DHCP Server Function

This topic details the lab activity for Lab 4-8.

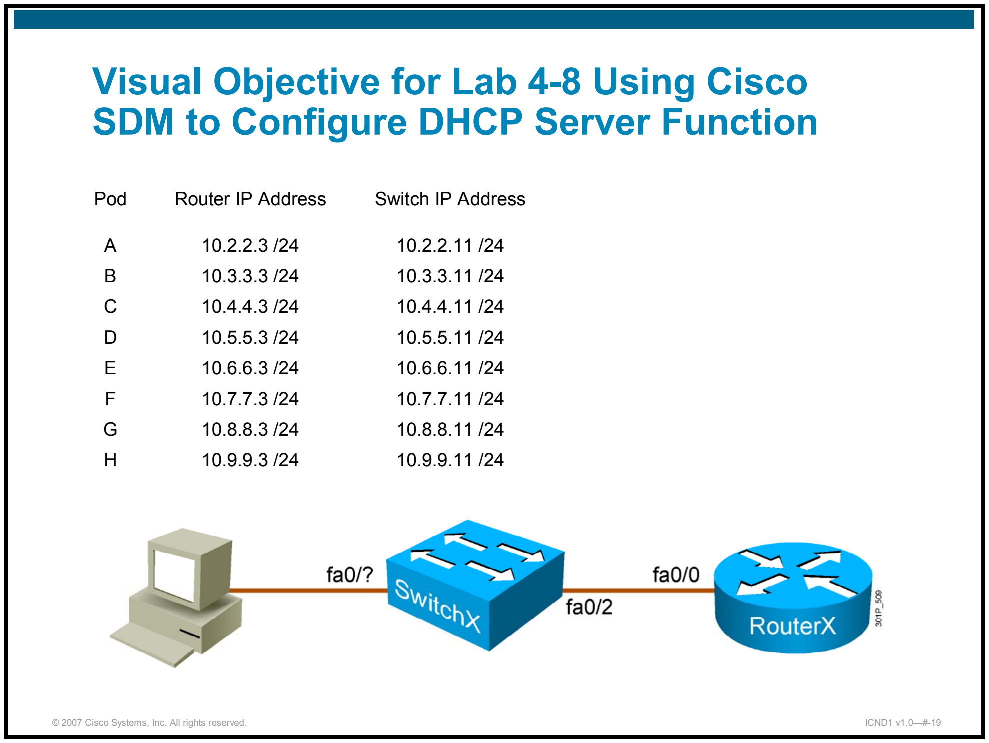
Objectives

You will complete these tasks in this lab:

- You will use Cisco SDM to configure a DHCP pool of addresses.
- You will use Cisco SDM to verify that at least one DHCP client has received an address from the pool just created.
- You will use Cisco IOS commands to locate the switch port through which the DHCP client attaches to your workgroup switch.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-8 Using Cisco SDM to Configure DHCP Server Function

Pod	Router IP Address	Switch IP Address
A	10.2.2.3 /24	10.2.2.11 /24
B	10.3.3.3 /24	10.3.3.11 /24
C	10.4.4.3 /24	10.4.4.11 /24
D	10.5.5.3 /24	10.5.5.11 /24
E	10.6.6.3 /24	10.6.6.11 /24
F	10.7.7.3 /24	10.7.7.11 /24
G	10.8.8.3 /24	10.8.8.11 /24
H	10.9.9.3 /24	10.9.9.11 /24

ICND1 v1.0—#-19

Setup

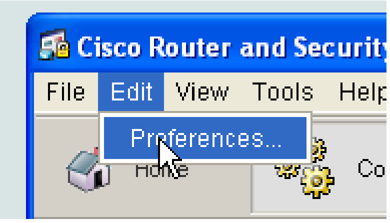
The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

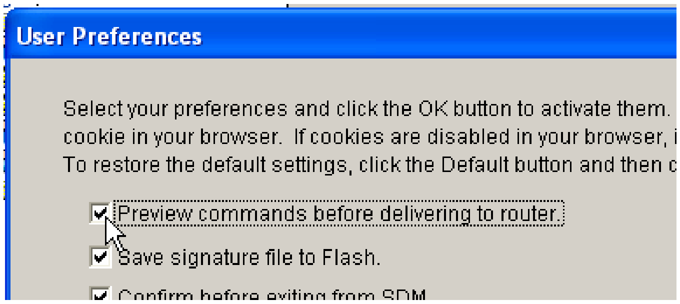
Instructor Notes

This lab uses Cisco SDM to configure the router as a DHCP server. In Task 1, the configuration is modified to allow the Cisco SDM login via a username and password locally configured. In Task 2, Cisco SDM is used to configure the router. In Task 3, the DHCP IP address is used to demonstrate how a MAC address can be traced to a specific switch port.

Optionally, you can have the learners modify Cisco SDM to show the CLI commands that are generated prior to sending to the router. To do this, go to **Edit > Preferences.**



Then click **Preview commands before delivering to router**.



Select your preferences and click the OK button to activate them.
cookie in your browser. If cookies are disabled in your browser, i
To restore the default settings, click the Default button and then c

☑ Preview commands before delivering to router.

☑ Save signature file to Flash.

☑ Confirm before exiting from SDM

Lab 4-9: Managing Remote Access Sessions

This topic details the lab activity for Lab 4-9.

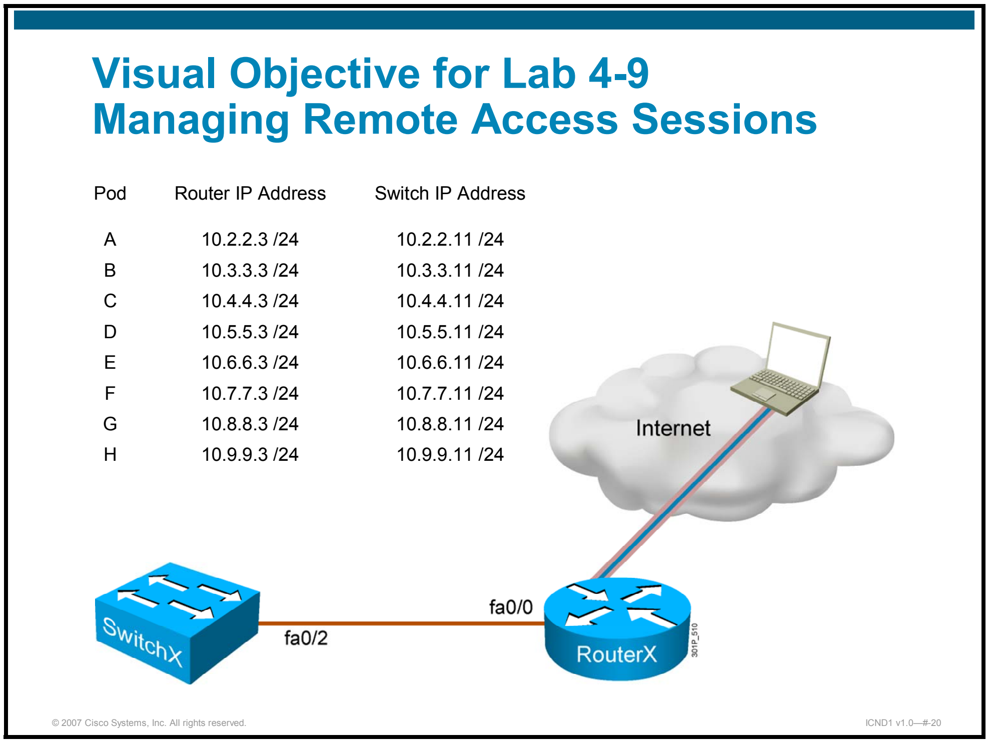
Objectives

You will complete these tasks in this lab:

- Initiate, suspend, resume, and close a Telnet session from a Cisco router or switch.
- Initiate, suspend, resume, and close an SSH session from a Cisco router or switch.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 4-9
Managing Remote Access Sessions

Pod	Router IP Address	Switch IP Address
A	10.2.2.3 /24	10.2.2.11 /24
B	10.3.3.3 /24	10.3.3.11 /24
C	10.4.4.3 /24	10.4.4.11 /24
D	10.5.5.3 /24	10.5.5.11 /24
E	10.6.6.3 /24	10.6.6.11 /24
F	10.7.7.3 /24	10.7.7.11 /24
G	10.8.8.3 /24	10.8.8.11 /24
H	10.9.9.3 /24	10.9.9.11 /24

© 2007 Cisco Systems, Inc. All rights reserved.   ICND1 v1.0—#-20

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-startup.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

The first task in this lab improves the usability of the CLI by increasing the history buffer size, logging synchronization, and so on.

In the second task, the learners connect via VPN so that they do *not* use the console server menus. This is necessary to prevent the menu system from intercepting the escape sequences that the learners will use in the task.

Common Issues

None known at this time.

Lab 5-1: Connecting to the Internet

This topic details the lab activity for Lab 5-1.

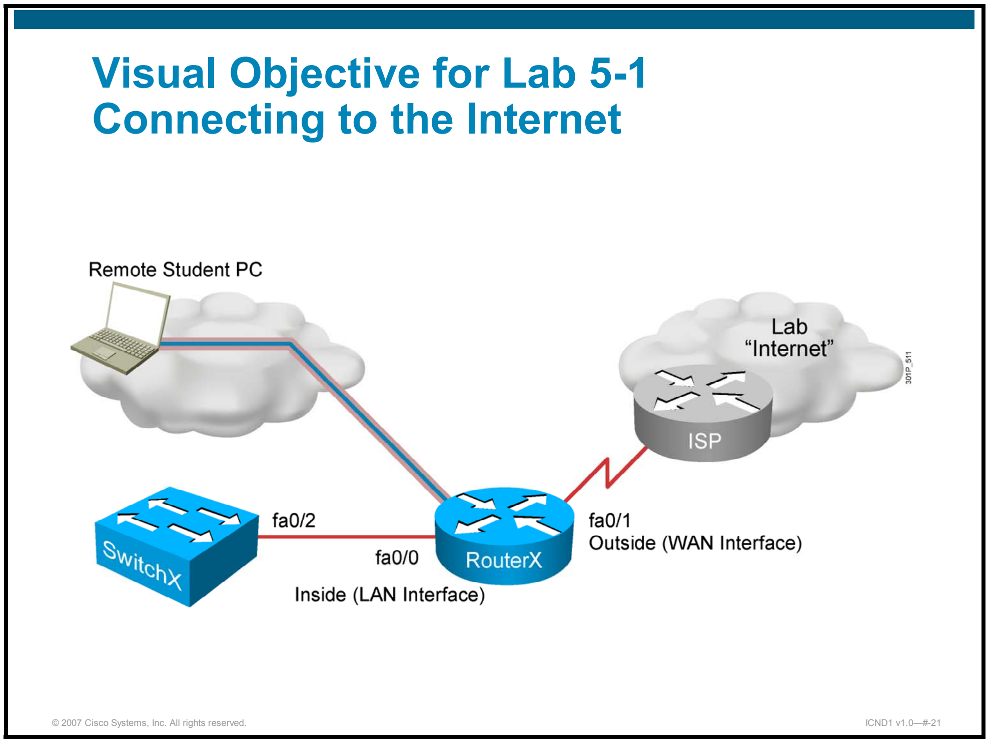
Objectives

You will complete these tasks in this lab:

- Use Cisco SDM to configure the WAN Ethernet interface to use a DHCP-obtained IP address.
- Use Cisco SDM to configure the router to support Port Address Translation of the inside Ethernet interface through the WAN Ethernet interface.
- Use Cisco SDM to verify that the configuration matches the requirements of the lab.
- Use the CLI to test and observe that PAT is taking place through the WAN Ethernet interface.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 5-1
Connecting to the Internet

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-21

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	**i1-corero-L5-1.txt**	**copy to running-config**
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

In this lab, Cisco SDM is used for configuring both the fa0/1 interface and for PAT. In Task 2, where the learners validate and observe PAT, it can seem confusing to the learners that they need to generate the ping from the workgroup switch, while the observation is done on the router.

Do not forget to apply the configuration change to the core router.

Common Issues

There are no known issues.

Lab 5-2: Connecting to the Main Office

This topic details the lab activity for Lab 5-2.

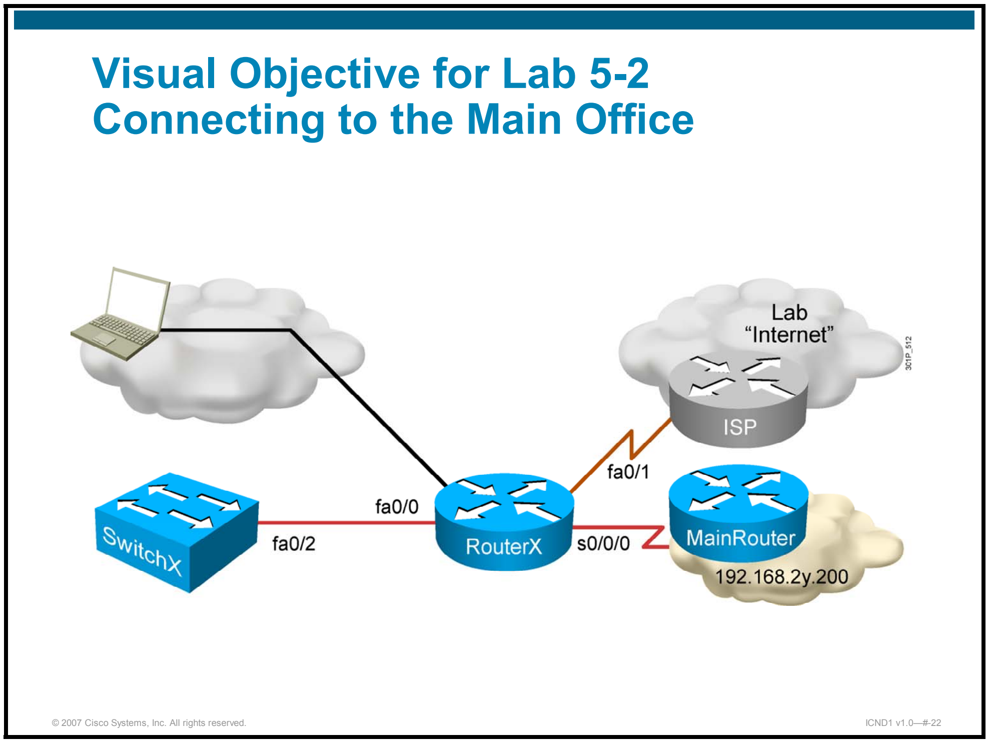
Objectives

You will complete these tasks in this lab:

- Configure your serial interface to use the PPP protocol.
- Configure your serial interface to use PPP CHAP authentication.
- Configure a static route to a given IP network, which can be reached via the serial interface.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 5-2
Connecting to the Main Office

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-22

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-L5-1.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

This lab is straightforward. You can take the opportunity to draw the attention of the learners to the administrative distance values for the gateway of last resort (254) and the static route (1).

Common Issues

There are no known issues.

Lab 5-3: Enabling Dynamic Routing to the Main Office

This topic details the lab activity for Lab 5-3.

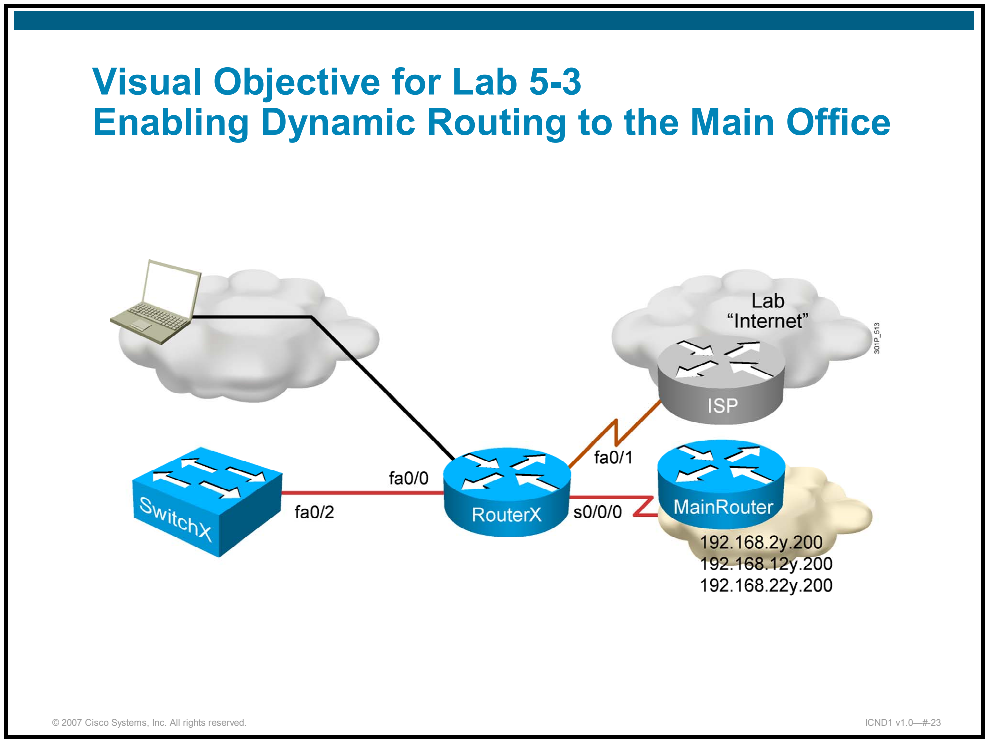
Objectives

You will complete these tasks in this lab:

- Configure RIP on your workgroup router.
- Verify that RIP is operating.
- Remove the unnecessary static route to an adjacent network.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 5-3
Enabling Dynamic Routing to the Main Office

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-23

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-L5-1.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

None.

Common Issues

There are no known issues.

Lab 6-1: Using Cisco Discovery Protocol

This topic details the lab activity for Lab 6-1.

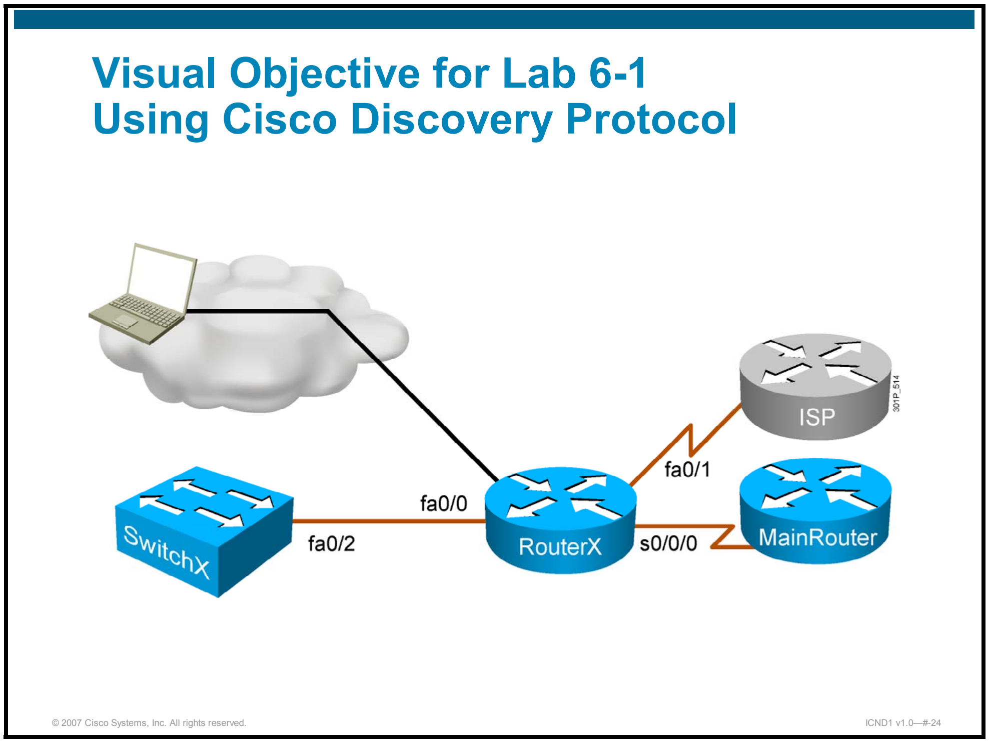
Objectives

You will complete these tasks in this lab:

- Verify that Cisco Discovery Protocol is running on your workgroup router and switch.
- Display information about neighboring Cisco devices.
- Limit which interfaces run Cisco Discovery Protocol, as a security measure.
- Verify your changes.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 6-1
Using Cisco Discovery Protocol

© 2007 Cisco Systems, Inc. All rights reserved. ICND1 v1.0—#-24

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-L5-1.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

None.

Common Issues

There are no known issues.

Lab 6-2: Managing Router Startup Options

This topic details the lab activity for Lab 6-2.

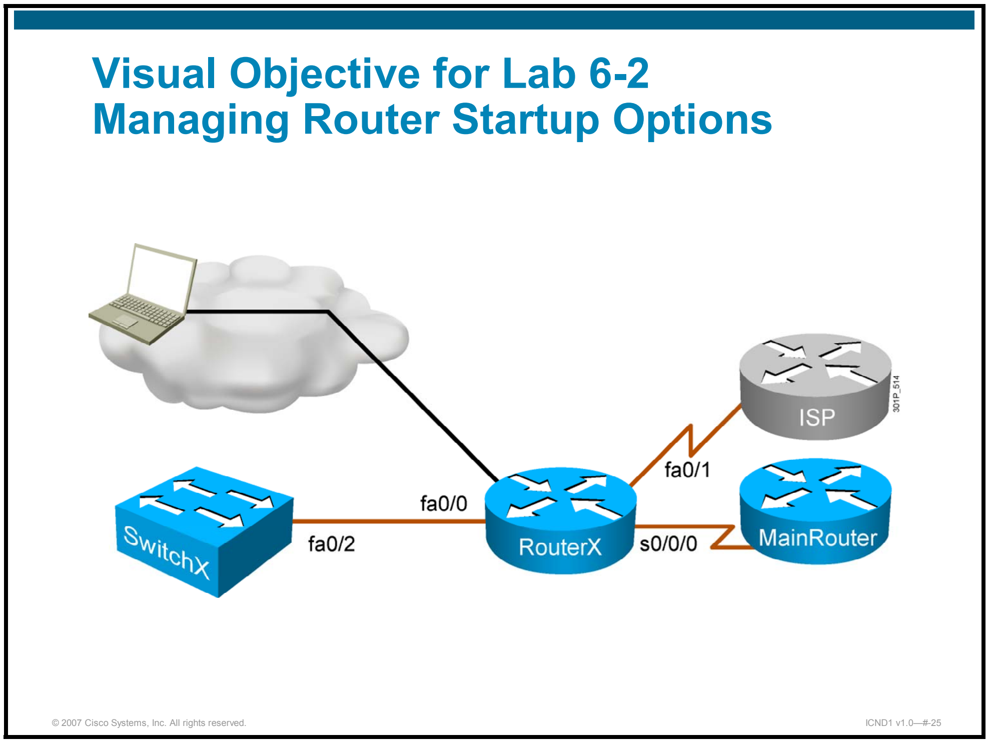
Objectives

You will complete these tasks in this lab:

- Display and modify the configuration register to a specified value and return it to its original value.
- Validate, by inspection of output, whether a displayed configuration in the startup-config file is from the running configuration or the startup configuration.
- Modify the sequence of Cisco IOS files loaded at startup, by providing a sequenced list of boot system commands.
- Observe a reload and verify which of the boot statements was processed to obtain the running Cisco IOS binary file.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 6-2
Managing Router Startup Options

ICND1 v1.0—#-25

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-L5-1.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab

Instructor Notes

Although Task 2 is written to avoid boot problems, you may want to ask the students to have you validate their boot system commands before they do a reload.

Common Issues

There are no known issues.

Lab 6-3: Managing Cisco Devices

This topic details the lab activity for Lab 6-3.

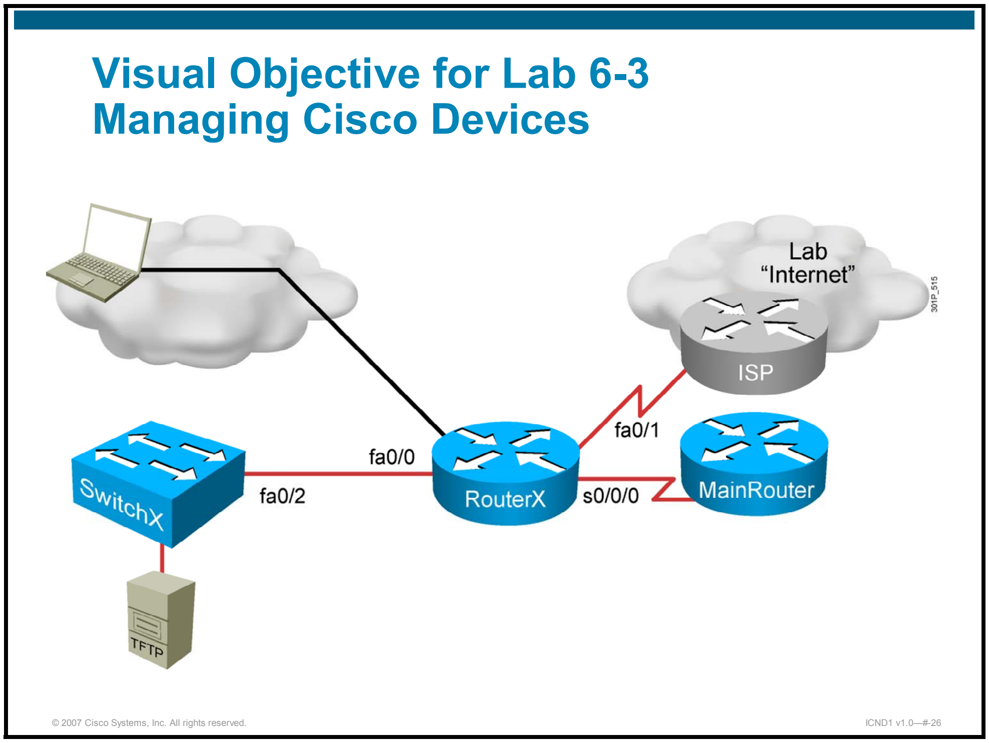
Objectives

You will complete these tasks in this lab:

- Save your running configuration on a remote TFTP server.
- Upload and download configuration files.
- Copy and delete files to local flash memory.
- Ensure that the router is lightly loaded before using debugging commands.
- Turn debugging on and off.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.



Visual Objective for Lab 6-3
Managing Cisco Devices

© 2007 Cisco Systems, Inc. All rights reserved.

ICND1 v1.0—#-26

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	i1-corero-L5-1.txt	same as previous lab
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	i1-coreswc-startup.txt	same as previous lab
VPNTS	vpnts-all.txt	same as previous lab
TFTP server	**descript-config**	**This small configuration element file should be available for download, as part of a lab task.**
TFTP server	**c2800nm-advipservicesk9-mz.124-12.bin**	**The IOS image file should be available for download, as part of a lab task.**

Instructor Notes

In Task 1, the learners copy files to the TFTP server. You should have *all* your configuration and Cisco IOS files write-protected (set as read-only) to avoid being overwritten accidentally.

In Task 2, the learners use **debug**. Because they have accessed the router via the console port, they are unaware that, if they enter via a vty session, they will not see any output until they use the **terminal monitor** command. The next revision of the course may include steps to do this.

Common Issues

There are no known issues.

Lab 6-4: Confirming the Reconfiguration of the Branch Network

This topic details the lab activity for Lab 6-4.

Objectives

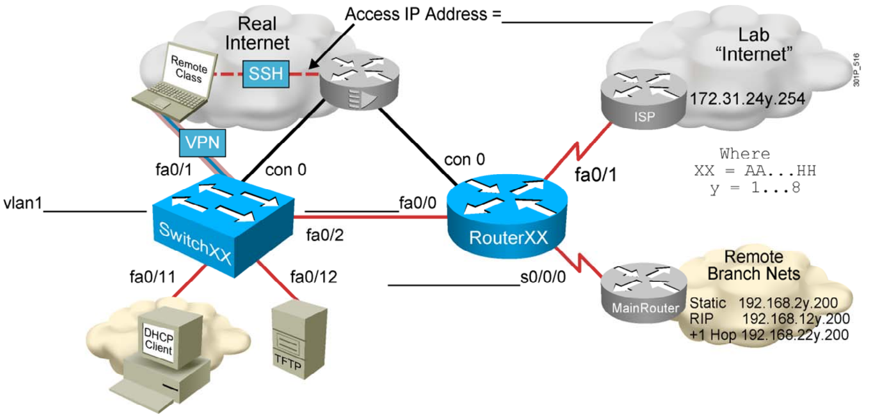
You will complete these tasks in this lab:

- Complete the reconfiguration of your assigned workgroup switch using information provided in the checklist below.
- Complete the reconfiguration of your workgroup router using information provided in the checklists.
- You will see the routes indicated in the visual object, after enabling dynamic routing on your workgroup router.
- You will perform tests to validate that your final configuration meets the new topology information.

Visual Objective

The figure displays the lab topology that you will use to complete this lab.

Visual Objective for Lab 6-4 Configuring the Reconfiguration of the Branch Network



ICND1 v1.0—#-27

Setup

The table describes how to set up lab configurations with equipment for this lab.

Device	Configuration File to Install	Configuration Instructions
CoreRouter	**i1-corero-L6-4.txt**	**copy to running config**
CoreSwitchA	i1-coreswa-all.txt	same as previous lab
CoreSwitchB	i1-coreswb-all.txt	same as previous lab
CoreSwitchC	**i1-coreswc-L6-4.txt**	**copy to running config**
VPNTS	vpnts-all.txt	same as previous lab
TFTP server	descript-config	same as previous lab
TFTP server	c2800nm-advipservicesk9-mz.124-12.bin	same as previous lab
Core switch C	**CoreswcLab6-4**	**copy to running config**
Switches A - H	**i1-switchxx**	**Copy from the tftp server into the startup configuration** and **reload** all workgroup switches**.**
Routers A - H	**i1-routerxx**	**Copy from the tftp server into the startup configuration** and **reload** all workgroup switches**.**

Because there are many files to be changed for this lab, you may want to change only the core configurations yourself, then have the learners download the configurations to their switches and routers and reload them.

Instructor Notes

The premise for this lab is that the students are taking over the configuration of a branch that has been partially configured. The configuration state is unknown to them and they need to complete it to the same level as they did their assigned workgroup. You should encourage them to view this as an opportunity to do troubleshooting, rather than just a repeat of the labs.

All the workgroup switches and routers are preconfigured from two base configurations. Because of anticipated time constraints, the switch configuration requires only a small amount of work.

The switch starting configuration requires the following corrections to be made:

- Hostname must be changed.
- IP address of VLAN 1 needs to match their assigned workgroup.
- IP Def gateway must match their assigned workgroup.

The routing configuration has only a few configuration elements from the final ending configuration. The learner will need to correct the following in order to function correctly:

- Hostname must be changed.
- The banner message must be changed because it welcomes anyone to access the device.
- The IP address of router fa0/0 must be changed.

In order to assist the learners, the lab is written with two worksheets to guide them. Most of the syntax is given to them and references are made to the location of the associated lab in the Lab Guide.

During the beta version, you can teach the timings for lab completion, between 105 to 180 minutes.

If, as you teach the class, you find that there is either too much or not enough time for a typical learner to complete the lab, you can modify the starting configurations, and in fact tailor them to meet your needs.

Common Issues

There are no known issues.

Configuration Files Summary

This topic details the course configuration files, which provide information about the starting condition of each lab.

Configuration Filename	Comments
i1-corero-startup.txt	Starting config.
i1-coreswa-all.txt	Configuration used in all labs.
i1-coreswb-all.txt	Configuration used in all labs.
i1-coreswc-startup.txt	Starting configuration.
vpnts-all.txt	Configuration used in all labs.
i1-corero-L5-1.txt	Enables interfaces on CoreRouter to support DHCP server for Lab 5-1. Enables interfaces on CoreRouter to support serial lines for Lab 5-2. Changes hostname on CoreRouter to MainRouter ready for Cisco Discovery Protocol in Lab 6-1.
descript-config	Configuration element used in Lab 6-3 to be uploaded by learners to their router.
i1-corero-L6-4.txt	Changes Serial 1/x IP addresses for Lab 6-4.
i1-coreswc-L6-4.txt	Changes VLANs used by VPN to match new addressing in Lab 6-4.
i1-routerxx.txt	Preload configurations AA-HH prior to Lab 6-4.
i1-switchxx.txt	Preload configurations AA-HH prior to Lab 6-4.

Lab Activity Solutions

Labs 1-1, 1-2, 1-3, and 2-1 had their answers within the labs and resulted in no configuration changes.

Lab 2-2 Answer Key: Performing Switch Startup and Initial Configuration

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
```

```
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 password sanjose
 no login
line vty 5 15
 password sanjose
 no login
!
end
```

Lab 2-3 Answer Key: Enhancing the Security of Initial Switch Configuration

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
 3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
 02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
 30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
 33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
 81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
 8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
 E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
 42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
 F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
 301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
 0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
 1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
 06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
 0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
 F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
 5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
 44531337 B03B7055 48A0B320 0A6C3173 C0
 quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/12
 switchport mode access
!
interface FastEthernet0/13
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 shutdown
!
interface FastEthernet0/19
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login ^C
********** Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 password 7 111A180B1D1D1809
 login
line vty 0 4
 password 7 111A180B1D1D1809
 login local
line vty 5 15
 password 7 111A180B1D1D1809
 login local
!
end
```

Lab 2-4 Answer Key: Operating and Configuring a Cisco IOS Device

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
  3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
  02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
  30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
  26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
  33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
  63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
  8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
  E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
  42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
  F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
  301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
  0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
  1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
  06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
  0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
  F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
  5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
  44531337 B03B7055 48A0B320 0A6C3173 C0
  quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/12
 switchport mode access
!
interface FastEthernet0/13
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 switchport mode access
 shutdown
!
interface FastEthernet0/19
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login ^C
**********  Warning  *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 password 7 111A180B1D1D1809
 login
line vty 0 4
 password 7 111A180B1D1D1809
 login local
line vty 5 15
 password 7 111A180B1D1D1809
 login local
!
end
```

Lab 4-1 Answer Key: Converting Decimal to Binary and Binary to Decimal

Task 1: Convert from Decimal Notation to Binary Format

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Decimal	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Binary**
48	0	0	1	1	0	0	0	0	48 = 32+16 = 00110000
146	1	0	0	1	0	0	1	0	146 = 128+16+2 = 10010010
222	1	1	0	1	1	1	1	0	222 = 128+64+16+8+4+2 = 1101110
119	0	1	1	1	0	1	1	1	119 = 64+32+16+4+2+1 = 01110111
135	1	0	0	0	0	1	1	1	135 = 128+4+2+1 = 10000111
60	0	0	1	1	1	1	0	0	60 = 32+16+8+4 = 00111100

Task 2: Convert from Binary Notation to Decimal Format

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11001100	1	1	0	0	1	1	0	0	128+64+8+4 = 204
10101010	1	0	1	0	1	0	1	0	128+32+8+2 = 170
11100011	1	1	1	0	0	0	1	1	128+64+32+2+1 = 227
10110011	1	0	1	1	0	0	1	1	128+32+16+2+1 = 179
00110101	0	0	1	1	0	1	0	1	32+16+4+1 = 53
10010111	1	0	0	1	0	1	1	1	128+16+4+2+1 = 151

Lab 4-2 Answer Key: Classifying Network Addressing

Task 1: Convert from Decimal IP Address to Binary Format

Step 1 Table to express 145.32.59.24 in binary format:

Base-2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Decimal	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Binary**
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59	0	0	1	1	1	0	1	1	00111011
24	0	0	0	1	1	0	0	0	00011000
Binary Format IP Address						10010001.00100000.00111011.00011000			

Step 2 Table to express 200.42.129.16 in binary format:

Base-2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Decimal	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Binary**
200	1	1	0	0	1	0	0	0	11001000
42	0	0	1	0	1	0	1	0	00101010
129	1	0	0	0	0	0	0	1	10000001
16	0	0	0	1	0	0	0	0	00010000
Binary Format IP Address						11001000.00101010.10000001.00010000			

Step 3 Table to express 14.82.19.54 in binary format:

Base-2	**2^7**	**2^6**	**2^5**	**2^4**	**2^3**	**2^2**	**2^1**	**2^0**	
Decimal	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Binary**
14	0	0	0	0	1	1	1	0	00001110
82	0	1	0	1	0	0	1	0	01010010
19	0	0	0	1	0	0	1	1	00010011
54	0	0	1	1	0	1	1	0	00110110
Binary Format IP Address						00001110.01010010.00010011.00110110			

Task 2: Convert from Binary Format to Decimal IP Address

Step 1 Table to express 11011000.00011011.00111101.10001001 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11011000	1	1	0	1	1	0	0	0	216
00011011	0	0	0	1	1	0	1	1	27
00111101	0	0	1	1	1	1	0	1	61
10001001	1	0	0	0	1	0	0	1	137
Decimal Format IP Address						216.27.61.137			

Step 2 Table to express 11000110.00110101.10010011.00101101 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11000110	1	1	0	0	0	1	1	0	198
00110101	0	0	1	1	0	1	0	1	53
10010011	1	0	0	1	0	0	1	1	147
00101101	0	0	1	0	1	1	0	1	45
Decimal Format IP Address						198.53.147.45			

Step 3 Table to express 01111011.00101101.01000011.01011001 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
01111011	0	1	1	1	1	0	1	1	123
00101101	0	0	1	0	1	1	0	1	45
01000011	0	1	0	0	0	0	1	1	67
01011001	0	1	0	1	1	0	0	1	89
Decimal Format IP Address						123.45.67.89			

Task 3: Identify IP Address Classes

Binary IP Address	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2^h-2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	2^{16}-2 = 65,534
11001000.00101010.10000001.00010000	200.42.129.16	Class C	24	2^{8}-2 = 254
00001110.01010010.00010011.00110110	14.82.19.54	Class A	8	2^{24}-2 = 16,777,214
11011000.00011011.00111101.10001001	216.27.61.137	Class C	24	2^{8}-2 = 254
10110011.00101101.01000011.01011001	179.45.67.89	Class B	16	2^{16}-2 = 65,534
11000110.00110101.10010011.00101101	198.53.147.45	Class C	24	2^{8}-2 = 254

Task 4: Identify Valid and Invalid Host IP Addresses

Decimal IP Address	Valid or Invalid	If Invalid, Indicate Reason
23.75.345.200	Invalid	"345" exceeds an 8-bit value (max=255)
216.27.61.134	Valid	
9102.54.94	Invalid	One octet is missing
255.255.255.255	Invalid	Valid number but is an administrative number that should not be assigned to a host
142.179.148.200	Valid	
200.42.129.16	Valid	
0.124.0.0	Invalid	A Class A address cannot use 0 as the first octet

Lab 4-3 Answer Key: Computing Usable Subnetworks and Hosts

Task 1: Determine the Number of Bits Required to Subnet a Class C Network

Given a Class C network address of 192.168.89.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
2	1	2^7-2 = 126
5	3	2^5-2 = 30
12	4	2^4-2 = 14
24	5	2^3-2 = 6
40	6	2^2-2 = 2

Task 2: Determine the Number of Bits Required to Subnet a Class B Network

Given a Class B network address of 172.25.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
5	3	2^{13}-2 = 8,190
8	3	2^{13}-2 = 8,190
14	4	2^{12}-2 = 4,094
20	5	2^{11}-2 = 2,046
35	6	2^{10}-2 = 1,022

Task 3: Determine the Number of Bits Required to Subnet a Class A Network

Given a Class A network address of 10.0.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
10	4	2^{20}-2 = 1,048,574
14	4	2^{20}-2 = 1,048,574
20	5	2^{19}-2 = 524,286
40	6	2^{18}-2 = 262,142
80	7	2^{17}-2 = 131,070

Lab 4-4 Answer Key: Calculating Subnet Masks

Task 1: Determine the Number of Possible Network Addresses

Classful Address	Decimal Subnet Mask	Binary Subnet Mask	Number of Hosts per Subnet (2^h-2)
/20	255.255.240.0	11111111.11111111.11110000.00000000	4,094
/21	255.255.248.0	11111111.11111111.11111000.00000000	2,046
/22	255.255.252.0	11111111.11111111.11111100.00000000	1,022
/23	255.255.254.0	11111111.11111111.11111110.00000000	510
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2

Task 2: Given a Network Block, Define Subnets

Assume that you have been assigned the 172.25.0.0 /16 network block. You need to establish eight subnets. Complete the following questions.

1. How many bits do you need to borrow to define 12 subnets? 4
2. Specify the classful address and subnet mask in binary and decimal that allows you to create 12 subnets.
   Classful address: /20
   Subnet mask (binary): 11111111.11111111.11110000.00000000
   Subnet mask (decimal): 255.255.240.0
3. Use the eight-step method to define the 12 subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0000 0000 ~~1111 0000~~

Step	Description	Example
4.	Copy the significant bits four times.	0000 0000 (first subnet) 0000 0001 (first host address) 0000 1110 (last host address) 0000 1111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0001 0000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.1.0 to 172.25.14.0	172.25.15.0
1	172.25.16.0	172.25.17.0 to 172.25.30.0	172.25.31.0
2	172.25.32.0	172.25.33.0 to 172.25.46.0	172.25.47.0
3	172.25.48.0	172.25.49.0 to 172.25.62.0	172.25.63.0
4	172.25.64.0	172.25.65.0 to 172.25.78.0	172.25.79.0
5	172.25.80.0	172.25.81.0 to 172.25.92.0	172.25.95.0
6	172.25.94.0	172.25.95 to 172.25.108.0	172.25.109.0
7	172.25.110.0	172.25.111.0 to 172.25.124.0	172.25.125.0

Task 3: Given Another Network Block, Define Subnets

Assume that you have been assigned the 192.168.1.0 /24 network block.

1. How many bits do you need to borrow to define six subnets? 3

2. Specify the classful address and subnet mask in binary and decimal that allows you to create six subnets.
   Classful address: /27
   Subnet mask (binary): 11111111.11111111.11111111.11100000
   Subnet mask (decimal): 255.255.255.224

3. Use the eight-step method to define the six subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11100000
3.	Draw a line to delineate the significant bits in the assigned IP address.	000 00000

Step	Description	Example
	Cross out the mask so that you can view the significant bits in the IP address.	~~111 00000~~
4.	Copy the significant bits four times.	000 00000 (first subnet) 000 00001 (first host address) 000 11110 (last host address) 000 11111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	001 00000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.1.0	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128	192.168.1.129 to 192.168.1.158	192.168.1.159
5	192.168.1.160	192.168.1.161 to 192.168.1.190	192.168.1.191

Task 4: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 192.168.111.0 /28 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111111.11110000
   Subnet mask (decimal): 255.255.255.240

2. How many subnets can you define with the specified mask? 16

3. How many hosts will be in each subnet? 14

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	10000001
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	1000 0001 ~~1111 0000~~

Step	Description	Example
4.	Copy the significant bits four times.	1000 0000 (first subnet) 1000 0001 (first host address) 1000 1110 (last host address) 1000 1111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	1001 0000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.111.0	192.168.111.1 to 192.168.111.126	192.168.111.127
1	192.168.111.128	192.168.111.129 to 192.168.111.142	192.168.111.143
2	192.168.111.144	192.168.111.145 to 192.168.111.158	192.168.111.159
3	192.168.111.160	192.168.111.161 to 192.168.111.174	192.168.111.175
4	192.168.111.176	192.168.111.177 to 192.168.111.190	192.168.111.191
5	192.168.111.192	192.168.111.193 to 192.168.111.206	192.168.111.207
6	192.168.111.208	192.168.111.209 to 192.168.111.222	192.168.111.223

Task 5: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.25.0.0 /23 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111110.00000000
   Subnet mask (decimal): 255.255.254.0

2. How many subnets can you define with the specified mask?
   126

3. How many hosts will be in each subnet?
   510

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	01110000.00000000
2.	Write the mask or classful prefix length in binary.	11111110.00000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0111000 0.00000000 ~~1111111 0.~~00000000

Step	Description	Example
4.	Copy the significant bits four times.	0111000 0.00000000 (first subnet) 0111000 0.00000001 (first host address) 0111000 1.11111110 (last host address) 0111000 1.11111111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0111001 0.00000000 (next subnet)

5. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.0.1 to 172.25.1.254	172.25.1.255
1	172.25.2.0	172.25.2.1 to 172.25.3.254	172.25.3.255
2	172.25.4.0	172.25.4.1 to 172.25.5.254	172.25.5.255
3	172.25.6.0	172.25.6.1 to 172.25.7.254	172.25.7.255
4	172.25.8.0	172.25.8.1 to 172.25.9.254	172.25.9.255
. . .			

Task 6: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.20.0.0 /25 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111111.10000000
   Subnet mask (decimal): 255.255.255.128

2. How many subnets can you define with the specified mask?
   510

3. How many hosts will be in each subnet?
   126

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000.10000001
2.	Write the mask or classful prefix length in binary.	11111111.10000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	1 0000001 ~~1 0000000~~

Step	Description	Example
4.	Copy the significant bits four times.	00000000.10000000 (first subnet) 00000000.10000001 (first host address) 00000000.11111110 (last host address) 00000000.11111111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	00000001.10000000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.20.0.0	172.20.0.1 to 172.20.0.126	172.20.0.127
1	172.20.0.128	172.20.0.129 to 172.20.0.254	172.20.0.255
2	172.20.1.0	172.20.1.1 to 172.20.1.126	172.20.1.127
3	172.20.1.128	172.20.1.129 to 172.20.1.254	172.20.1.255
4	172.20.2.0	172.20.2.1 to 172.20.2.126	172.20.2.127
5	172.20.2.128	172.20.2.129 to 172.20.2.254	172.20.2.255
. . .			

Lab 4-5 Answer Key: Performing Initial Router Startup

When you complete this activity, your workgroup switch will have no configuration. Displayed here is the output of the erase startup-config. Remember the username/password of cisco/cisco comes from the default Cisco SDM configuration. Your output will be similar to the results here:

```
Username: cisco
Password:
yourname#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
yourname#
*Mar 13 17:28:00.003: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
yourname#reload
Proceed with reload? [confirm]

*Mar 13 17:28:07.939: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload Command.

System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.

Initializing memory for ECC
.
c2811 platform with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled


Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0x228d9f8
Self decompressing the image :
##############################################################################
##############################################################################
########################################### [OK]

Smart Init is enabled
smart init is sizing iomem
  ID            MEMORY_REQ            TYPE
0003E7          0X003DA000 C2811 Mainboard
                0X00263F50 Onboard VPN
                0X000021B8 Onboard USB
                0X002C29F0 public buffer pools
                0X00211000 public particle pools
TOTAL:          0X00B13AF8

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
configuration or there is a software problem and
system operation may be compromised.
Rounded IOMEM up to: 12Mb.
Using 4 percent iomem. [12Mb/256Mb]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
```

```
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
Image text-base: 0x40093160, data-base: 0x42B00000


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2811 (revision 49.46) with 249856K/12288K bytes of memory.
Processor board ID FTX1050A3Q6
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!

sslinit fn

*Mar 13 17:29:36.819: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State
changed to: Initialized
*Mar 13 17:29:36.819: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State
changed to: Enabled
*Mar 13 17:29:38.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-
Null0, changed state to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
to up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to
up
*Mar 13 17:29:38.087: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to
down
```

```
*Mar 13 17:29:39.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
*Mar 13 17:29:39.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
*Mar 13 17:29:41.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
*Mar 13 17:29:41.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Mar 13 17:30:04.463: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
*Mar 13 17:30:07.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
*Mar 13 17:31:02.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down
*Mar 13 17:31:44.471: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
*Mar 13 17:31:44.475: %LINK-5-CHANGED: Interface Serial0/0/1, changed state to
administratively down
*Mar 13 17:31:44.491: %IP-5-WEBINST_KILL: Terminating DNS process
*Mar 13 17:31:45.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
*Mar 13 17:31:45.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar 13 17:31:46.007: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
*Mar 13 17:31:46.011: %SNMP-5-COLDSTART: SNMP agent on host Router is
undergoing a cold start
*Mar 13 17:31:46.219: %SYS-6-BOOTTIME: Time taken to reboot after reload =
216 seconds
*Mar 13 17:31:46.399: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
```

Lab 4-6 Answer Key: Performing Initial Router Configuration

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password cisco
!
no aaa new-model
!
!
ip cef
!
!
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
no ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 password sanjose
 login
!
scheduler allocate 20000 1000
!
end
```

Lab 4-7 Answer Key: Enhancing the Security of the Initial Router Configuration

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username netadmin password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
no ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 password 7 14041305060B392E
 login
line aux 0
line vty 0 4
 password 7 071C204244060A00
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 4-8 Answer Key: Using Cisco SDM to Configure DHCP Server Function

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
```

```
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
```

```
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 password 7 14041305060B392E
 login
line aux 0
line vty 0 4
 password 7 071C204244060A00
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 4-9 Answer Key: Managing Remote Access Sessions

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
```

```
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
```

```
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 5-1 Answer Key: Connecting to the Internet

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
!
!
ip http server
ip http authentication local
ip http secure-server
!
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
```

```
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 5-2 Answer Key: Connecting to the Main Office

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
```

```
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip route 192.168.21.0 255.255.255.0 10.140.10.1
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
```

```
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 5-3 Answer Key: Enabling Dynamic Routing to the Main Office

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
```

```
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
```

```
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 6-1 Answer Key: Using Cisco Discovery Protocol

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.4
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.dET$BDxkofHF3aAsRthe/c0.c.
enable password 7 14141B180F0B
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 082F495A081D081E1C
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
```

```
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 14041305060B392E
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 071C204244060A00
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchX
!
enable secret 5 $1$A11O$0z83HwmswM/vk5.RSZpVr.
enable password 7 05080F1C2243
!
username netadmin password 7 030A5E1F070B2C4540
no aaa new-model
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-1833200768
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1833200768
 revocation-check none
 rsakeypair TP-self-signed-1833200768
!
!
```

```
crypto ca certificate chain TP-self-signed-1833200768
 certificate self-signed 01
  3082028D 308201F6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  53312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31383333 32303037 36383120 301E0609 2A864886 F70D0109
  02161177 675F7377 5F612E63 6973636F 2E636F6D 301E170D 39333033 30313030
  30313033 5A170D32 30303130 31303030 3030305A 3053312F 302D0603 55040313
  26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D313833
  33323030 37363831 20301E06 092A8648 86F70D01 09021611 77675F73 775F612E
  63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 8100B444 4F07E979 88953526 E0B8480C 52DBC1E7 E5FF660A 41932329
  8FB4A8EE 142FAEC4 744CB8BE 021BDAE5 BF005CA6 99D0BDC7 68C4A873 25A2F06C
  E460FAE5 1435B900 43505E02 3F0F5E4B D61D6787 59B6AE32 13558C75 561A6BB0
  42C15C96 D078A449 669E4B58 CD5857D0 1B570F43 008B811F 45CD05B0 50D144BA
  F83865F5 8BFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF
  301C0603 551D1104 15301382 1177675F 73775F61 2E636973 636F2E63 6F6D301F
  0603551D 23041830 16801414 679B7C0E C82E65FB 8953EC84 1FC9DD49 E672A630
  1D060355 1D0E0416 04141467 9B7C0EC8 2E65FB89 53EC841F C9DD49E6 72A6300D
  06092A86 4886F70D 01010405 00038181 006C7E92 A7F96199 D1D81ADA FA16C868
  0660013D 4A91A319 6D6DBD61 B5147AAA FF0FCF26 3DF20CA7 9694B3B8 24ABBEAC
  F8942F5F E53466BB 04E12200 25432AFE A09DDFCF A07A5A4A 145BE58D 4040040A
  5B085A4E 895C45BC 4DF264BC BFE32124 F4AA3BDB B9CF2CC2 35F3B42A B16BFD69
  44531337 B03B7055 48A0B320 0A6C3173 C0
  quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be01
 switchport port-security mac-address sticky 001a.2fe7.3089
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/4
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/5
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/6
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/7
 switchport mode access
 shutdown
 no cdp enable
```

```
!
interface FastEthernet0/8
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/9
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/10
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/11
 switchport mode access
 no cdp enable
!
interface FastEthernet0/12
 switchport mode access
 no cdp enable
!
interface FastEthernet0/13
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/14
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/15
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/16
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/17
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/18
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/19
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/20
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/21
 switchport mode access
 shutdown
 no cdp enable
```

```
!
interface FastEthernet0/22
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/23
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/24
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
 no cdp enable
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 111A180B1D1D1809
 logging synchronous
 login
 history size 100
line vty 0 4
 password 7 111A180B1D1D1809
 logging synchronous
 login local
 history size 100
line vty 5 15
 password 7 111A180B1D1D1809
 logging synchronous
 login local
 history size 100
!
end
```

Lab 6-2 Answer Key: Managing Router Startup Options

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterX
!
boot-start-marker
boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.10.10.1
boot system flash c2800nm-advipservicesk9-mz.124-12.bin
boot system flash
boot-end-marker
!
no logging buffered
enable secret 5 $1$X.GH$OkseupwTuqqjGp4oP4Fdg0
enable password 7 121A0C041104
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool wgA_clients
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.3
   lease 0 0 5
!
!
no ip domain lookup
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3715519608
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3715519608
 revocation-check none
 rsakeypair TP-self-signed-3715519608
!
```

```
!
crypto pki certificate chain TP-self-signed-3715519608
 certificate self-signed 01
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373135 35313936 3038301E 170D3037 30343035 32333135
  30305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37313535
  31393630 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D0D2 4D67CC33 F0966C60 96BD12D2 675EB867 42087A6F 4310110E 1E852852
  E965291B A9E21580 7F77960A B83618A5 65A718BE 4E81DB21 669B48D1 172E1FF3
  73575C54 6B25A849 6E886C49 3EA0D03C CC5E7AFA 186AE594 22F612D6 8CA089EC
  355AFCF5 9FBA492A EEEB13C8 27A6F2BE EEC51E85 18B52144 10DDA46C C0831824
  D0450203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 1177675F 726F5F61 2E636973 636F2E63 6F6D301F 0603551D
  23041830 168014B7 CBDB7C0C C2AEB57B B2CA8F85 6C9567DA ACA8F430 1D060355
  1D0E0416 0414B7CB DB7C0CC2 AEB57BB2 CA8F856C 9567DAAC A8F4300D 06092A86
  4886F70D 01010405 00038181 0061FD2F C903A4A2 0E241513 68AD17EA 16856A52
  46C655CA 7AD9C703 DE996CD7 7F009ED1 19829639 6D57B06C 5225DEF4 5F3325D1
  1567E90F 60858412 AB1E106A 3110FD46 9439D60A 7FFB783D D740FDAC EC00C4B5
  388FFD58 436F2B2A A305F71B 00E91CAD 90B5F317 D705450E DC511A46 E777ACAC
  1C07F960 64CCE156 F65330FE 02
  quit
username netadmin privilege 15 password 7 0208014F0A02022842
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex half
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 description Link to Main Office
 ip address 10.140.10.2 255.255.255.0
 encapsulation ppp
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
 version 2
 network 10.0.0.0
!
!
!
ip http server
ip http authentication local
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
```

```
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
dialer-list 1 protocol ip permit
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login ^C
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************^C
!
line con 0
 exec-timeout 60 0
 password 7 051807012B435D0C
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 password 7 051807012B435D0C
 logging synchronous
 login local
 history size 100
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab 6-3 Answer Key: Managing Cisco Devices

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
There were no overall changes to the configuration.!
```

Lab 6-4 Answer Key: Confirming the Reconfiguration of the Branch Network

When you complete this activity, your workgroup switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RouterXX
!
boot-start-marker
boot system flash c2800nm-advipservicesk9-mz.124-12.bin
boot system tftp c2800nm-advipservicesk9-mz.124-12.bin 10.10.10.1
boot system flash
boot-end-marker
!
enable secret 5 $1$t7tb$L8Par/.s/MaoshaZH1cLq0
enable password 7 0822455D0A16
!
no aaa new-model
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.149
ip dhcp excluded-address 10.10.10.200 10.10.10.254
!
ip dhcp pool branchXX-clients
   import all
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.3
   lease 0 0 5
!
!
ip domain name cisco.com
ip ssh version 2
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
crypto pki trustpoint TP-self-signed-3575601183
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3575601183
 revocation-check none
 rsakeypair TP-self-signed-3575601183
!
!
crypto pki certificate chain TP-self-signed-3575601183
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33353735 36303131 3833301E 170D3037 30353034 32313439
  31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 35373536
  30313138 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100E3CA 6B4F5C16 545F1796 C3600BE9 433F7C87 CB676A33 D42BF42A A6433BAF
  25582787 6028AE73 F3EAFD24 EA37AFEE CF6F101D 14EF2CCF 8EF4085C 2ED0E54B
  E1758915 13A5499E 378275C7 3BBE4F32 009DB10E 5039EB40 2C43D4EA 1407B634
  A0EFEB26 23E4045E EAFE99BE 88C4DA01 357684AC 65572494 ABDC6A99 AA85D645
  D8530203 010001A3 67306530 0F060355 1D130101 FF040530 030101FF 30120603
  551D1104 0B300982 07526F75 74657258 301F0603 551D2304 18301680 14E0035D
  916FE499 69EDA5C0 C15FDB83 17F62591 45301D06 03551D0E 04160414 E0035D91
  6FE49969 EDA5C0C1 5FDB8317 F6259145 300D0609 2A864886 F70D0101 04050003
  81810070 7B5F8CB1 BB014CBA 3E317573 C2303187 3534E5C7 71FDDDE5 EC4D6331
  A0498B71 49FE6A9A 5A5F6703 091EBDDC B828F955 4851F005 B214B407 4A0E67C0
  87AC8E94 52F130E9 73E28BD9 EC4A028B 6424BCF2 EF0A993C 1BA75BED E3E0D217
  E1129982 E1A40C9C 98F43F91 363474F2 97E3BBFF E60A7AA5 01327A27 EA69FCE6
0C4D36
  quit
username netadmin privilege 15 password 7 0505031B2048430017
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.10.10.3 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $ETH-WAN$
 ip address dhcp client-id FastEthernet0/1
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Serial0/0/0
 ip address 10.140.100.2 255.255.255.0
 encapsulation ppp
 no cdp enable
!
interface Serial0/0/1
 no ip address
 shutdown
 no cdp enable
!
router rip
 version 2
 network 10.0.0.0
!
!
```

```
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark INSIDE_IF=FastEthernet0/0
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.10.0 0.0.0.255
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner login □
************* Warning **********************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.
**************************************************************□
!
line con 0
 exec-timeout 60 0
 password 7 08324D4003161612
 logging synchronous
 login
 history size 100
line aux 0
line vty 0 4
 logging synchronous
 login local
 history size 100
 transport input ssh
!
scheduler allocate 20000 1000
!
end

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname SwitchXX
!
enable secret 5 $1$LLvt$3gBuRQzm6eAcGfQjsgHC01
enable password 7 01100F175804
!
username netadmin privilege 15 password 7 1419171F0D0027222A
no aaa new-model
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
ip ssh version 2
!
!
crypto pki trustpoint TP-self-signed-809024768
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-809024768
 revocation-check none
 rsakeypair TP-self-signed-809024768
!
!
crypto ca certificate chain TP-self-signed-809024768
 certificate self-signed 01
  3082028B 308201F4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  52312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 38303930 32343736 38312030 1E06092A 864886F7 0D010902
  16115377 69746368 582E6369 73636F2E 636F6D30 1E170D39 33303330 31303030
  3130305A 170D3230 30313031 30303030 30305A30 52312E30 2C060355 04031325
  494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 38303930
  32343736 38312030 1E06092A 864886F7 0D010902 16115377 69746368 582E6369
  73636F2E 636F6D30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
  02818100 D2D79D92 1395A6CB 46CAAD3C 6873B3D3 75B1B226 1E4EC5BC 87906C24
  DAC40D83 6380CE06 C04AE1DE B6DBD7A4 5941D5E5 C2FA7464 DC6135A6 EFED87E4
  966DC533 6BB18EDF 213503E7 B5B0E919 99C666B9 89AB8988 553288C0 400D6821
  912B2908 B076FE8D 4645B79C 1FDEEBEF 83DBB7AF 3C92B363 52F68131 E2BEEDC3
  4E0CC8FB 02030100 01A37130 6F300F06 03551D13 0101FF04 05300301 01FF301C
  0603551D 11041530 13821153 77697463 68582E63 6973636F 2E636F6D 301F0603
  551D2304 18301680 14B5A18A 31CE43E7 9D9704B4 815246B1 3D601AB8 A7301D06
  03551D0E 04160414 B5A18A31 CE43E79D 9704B481 5246B13D 601AB8A7 300D0609
  2A864886 F70D0101 04050003 81810007 16DD332F F2711854 434842FA 026C6F29
  82718220 8249778B 4CDFFE66 1B52B55E AA6BC328 CF0CD466 E9DE6464 CF1836A3
  F62723B8 14D8A873 535C205E BDC26BAC E73C448D 0E0B8194 402C6A67 CD6EFA78
  CDD0A83A 0335EB3E 9ADCA41E 768FA332 572AE050 1121207E D4E79437 894E3588
  65E3D60A 57150B63 9206A35B C71BB9
  quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0017.5a78.be0f
 switchport port-security mac-address sticky 001a.2fe7.3089
 no cdp enable
!
interface FastEthernet0/2
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/4
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/5
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/6
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/7
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/8
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/9
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/10
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/11
 switchport mode access
 no cdp enable
!
interface FastEthernet0/12
 switchport mode access
 no cdp enable
!
interface FastEthernet0/13
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/14
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/15
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/16
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/17
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/18
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/19
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/20
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/21
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/22
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/23
 switchport mode access
 shutdown
 no cdp enable
!
interface FastEthernet0/24
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
 no cdp enable
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
 no cdp enable
!
interface Vlan1
 ip address 10.10.10.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.3
ip http server
ip http secure-server
!
control-plane
!
banner login □
**********  Warning   *************
Access to this device is restricted to authorized persons only!
Un-authorized access is prohibited. Violators will be prosecuted.

**************************************************************□
!
line con 0
 exec-timeout 60 0
 password 7 04480A08052E5F4B
 logging synchronous
 login
 history size 100
line vty 0 4
 password 7 03175A01091C24
 logging synchronous
 login local
 history size 100
 transport input ssh
line vty 5 15
 password 7 001712080E541803
 logging synchronous
 login local
 history size 100
 transport input ssh
!
end
```

Teardown and Restoration

This topic describes how to tear down and restore the equipment that is used in the course.

Step 1 Workgroup Routers: Verify workgroup router flash: and remove descript-config (should have been deleted per Lab 6-3, Task 1, Step 26).

Step 2 Workgroup Routers: Copy flash:sdmconfig-2811.txt to startup-config, reload.

Step 3 Workgroup Switches: Erase startup and reload.

Step 4 Core Switch C: Copy tftp startup, file i1-coreswc-startup.txt, reload.

Step 5 Core Router: Copy tftp startup, file c1ro-startup.txt, reload.

Delta Information for *Interconnecting Cisco Networking Devices Part 1* v1.0

This document provides a summary of the differences between *Introduction to Cisco Networking Technologies (*INTRO) v2.1 and *Interconnecting Cisco Networking Devices Part 1* (ICND1) v1.0.

Course Goal

Upon completing the *Interconnecting Cisco Networking Devices Part 1* course, the learner should have the knowledge and skills necessary to install, operate, and troubleshoot a small branch office enterprise network, including connecting to a WAN and implementing network security.

ICND Prerequisite Skills and Knowledge

To fully participate in the *Interconnecting Cisco Networking Devices Part 1* course, learners should enter the course with at least these competencies:

- Basic computer literacy, including the use of general office software such as Microsoft Word and Microsoft Excel
- Basic Windows navigation and keyboard literacy skills
- Basic Internet usage skills
- Basic e-mail usage skills

Job Skills Taught

The course objectives were derived from the task list:

- Describe the operation of data networks
- Describe the purpose and functions of various network devices
- Select the components required to meet a given network specification
- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- Describe common networking applications, including web applications
- Describe the purpose and basic operation of the protocols in the OSI and TCP models
- Describe the implementation of Voice Over IP in a small network
- Interpret network diagrams
- Determine the path between two hosts across a network
- Describe the components required for network and Internet communications
- Identify and correct common network problems at Layers 1, 2, 3, and 7 using a layered model approach
- Differentiate between LAN and WAN operations and features
- Implement a small switched network

- Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- Explain the technology and media access control method for Ethernet technologies
- Explain network segmentation and basic traffic management concepts
- Explain the operation of Cisco switches and basic switching concepts
- Perform, save, and verify initial switch configuration tasks, including remote access management
- Verify network status and switch operation using basic utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig), **show** and **debug** commands
- Implement and verify port security
- Identify and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures
- Implement an IP addressing scheme and IP services to meet network requirements
- Describe the need and role of addressing in a network
- Create and apply an addressing scheme to a network
- Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment
- Describe, configure, and verify NAT
- Describe and verify DNS operation
- Describe the operation and benefits of using private and public IP addressing
- Explain the operation and benefits of using NAT, DHCP, and DNS
- Configure, verify, and troubleshoot DHCP operation on a router
- Implement static and dynamic addressing services for hosts in a LAN environment
- Configure a device to support NAT and DHCP
- Identify and correct IP addressing issues
- Implement a small routed network
- Describe basic routing concepts (packet forwarding, router lookup)
- Describe the operation of Cisco routers (router boot process, POST, router components)
- Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
- Configure, verify, and troubleshoot RIPv2
- Access and use the router CLI to set basic parameters
- Connect, configure, and verify operation status of a device interface
- Verify device configuration and network connectivity using ping, traceroute, Telnet, SSH, or other utilities
- Perform and verify routing configuration tasks for a static or default route given specific routing requirements
- Manage Cisco IOS configuration files (save, edit, upgrade, restore)
- Manage Cisco IOS Software

- Implement password and physical security
- Verify network status and router operation using basic utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig), **show** and **debug** commands
- Install a small wireless network
- Describe standards associated with wireless media (802.11a/b/g/n, Wi-Fi)
- Identify and describe the purpose of the components in a small wireless network
- Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
- Describe wireless security concerns and explain how to configure WPA security (open, WEP, WPA-1/2)
- Identify common issues with implementing wireless networks
- Identify security threats to a small network and describe general methods to mitigate those threats
- Explain increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats
- Explain general methods to mitigate common security threats to network devices, hosts, and applications
- Describe the functions of common security appliances and applications
- Describe security recommended practices including initial steps to secure network devices
- Describe VPN technology (importance, benefits, role, impact, components)
- Identify VPN client issues

Lesson and Lab Objectives

This table provides a comparison of the lesson and lab objectives for each module.

- MIN = Existing content, only *minor* edits.
- MAJ = Existing content from other courses, *major* edits to existing ICND content.
- NEW = New content and not from any other course.

Module	Lesson	Title	Source	Comments
0	0	Course Introduction	INTRO21S00.doc	
1	0	Building a Simple Network	INTRO21S01L00.doc	
1	1	Exploring the Functions of Networking	INTRO21S01L01.doc	Most of the content came from INTRO21S01L01.doc. New material is related to interpreting a network diagram, Impact of user applications on the network, and connection to the Internet.
1	2	Securing the Network	New Content	
1	3	Understanding the Host-to-Host Communications Model	INTRO21S01L03.doc	
1	4	Understanding the TCP/IP Internet Layer	INTRO21S04L03.doc	New contented was added on a DHCP and DNS overview.
1	5	Understanding the TCP/IP Transport Layer	INTRO21S06L01.doc	Two lessons from INTRO were combined into a single lesson.
			INTRO21S04L02.doc	
1	6	Exploring the Packet Delivery Process (This will be at a high level focusing on peer-to-peer)	New Content	This is a new lesson where a data exchange between two directly connected hosts is used to review the content covered to this point in the course.
1	Lab 1-1	Lab 1-1: Using Windows Applications as Network Tools	New	
1	Lab 1-2	Lab 1-2: Observing the TCP Three-Way Handshake	New	
1	Lab 1-3	Lab 1-3: Observing Extended PC Network Information	New	
1	7	Understanding Ethernet	INTRO21S02L01.doc	Two lessons from INTRO were combined into a single lesson.
			INTRO21S02L02.doc	
1	8	Connecting to an Ethernet LAN	INTRO21S02L03.doc	
2	0	Ethernet (LANs	INTRO21S03L00.doc	
2	1	Understanding the Challenges of Shared LANs	INTRO21S03L02.doc	
2	2	Solving Network Challenges with Switched LAN Technology	INTRO21S03L03.doc	

Module	Lesson	Title	Source	Comments
2	3	Exploring the Packet Delivery Process	New	This is a new lesson that builds on Lesson 6 of Module 1. A data exchange between host is used to review the content covered to this point in the course. However, this time the exchange is through a switch.
2	4	Operating Cisco IOS Software	INTRO21S08L01.doc	Two lessons from INTRO were combined into a single lesson.
			INTRO21S08L04.doc	
2	5	Starting a Switch	INTRO21S08L02.doc	
			ICND23S01L04.doc	MAC Address Table Management
2	Lab 2-1	Lab 2-1: Connecting to Remote Lab Equipment	New	
2	Lab 2-2	Lab 2-2: Performing Switch Startup and Initial Configuration	New	
2	6	Understanding Switch Security	INTRO21S08L04.doc	This is a new lesson that groups all of the switch security content into a single lesson. Much of this lesson is based upon content from INTRO21S08L04. However, new content has been added on SSH and securing unused switch ports.
2	Lab 2-3	Lab 2-3: Enhancing the Security of Initial Switch Configuration	New	
2	Lab 2-4	Lab 2-4: Operating and Configuring a Cisco IOS Device	New	
2	7	Maximizing the Benefits of Switching	INTRO21S03L04.doc	
2	8	Troubleshooting Switch Issues	New	This is a new lesson that was added to address troubleshooting common switch issues.
3	0	Wireless LANs	New	
3	1	Exploring Wireless Networking	New	This is a new lesson that provides an overview of WLANs.
3	2	Understanding WLAN Security	New	This is a new lesson that provides an overview of WLAN security.
3	3	Implementing a WLAN	New	This is a new lesson that provides an overview of WLAN implementations.

Module	Lesson	Title	Source	Comments
4	0	LAN Connections	INTRO21S04L00.doc	
4	1	Exploring the Functions of Routing	INTRO21S04L04.doc	
4	2	Understanding Binary Basics	INTRO21S05L01.doc	
4	3	Constructing a Network Addressing Scheme	INTRO21S05L03.doc	Two lessons from INTRO were combined into a single lesson.
			INTRO21S05L04.doc	
4	4	Starting a Cisco Router	INTRO21S08L03.doc	
4	Lab 4-1	Lab 4-1: Converting Decimal to Binary and Binary to Decimal		
4	5	Configuring a Cisco Router	INTRO21S08L04.doc	
4	Lab 4-2	Lab 4-2: Classifying Network Addressing		
4	6	Exploring the IP Packet Delivery Process	New	This is a new lesson that builds on Lesson 6 of Module 1 and Lesson 4 of Module 2. A data exchange between host is used to review the content covered to this point in the course. However, this time the exchange is through a router.
4	Lab 4-3	Lab 4-3: Computing Usable Subnetworks and Hosts	New	
4	7	Understanding Cisco Router Security	New	This is a new lesson that groups all of the switch security content into a single lesson. Much of this lesson is based upon content from INTRO21S08L04. However, new content has been added on SSH.
4	Lab 4-4	Lab 4-4: Calculating Subnet Masks	New	
4	8	Using Cisco SDM	SNRS10S07L01.doc	This a new lesson that introduces Cisco SDM.
4	9	Using a Cisco Router as a DHCP Server	New	This is a new lesson that covers using Cisco SDM to enable a DHCP server on the router.
4	Lab 4-5	Lab 4-5: Performing Initial Router Startup	New	
4	10	Accessing Remote Devices		INTRO21S09L02.doc
4	Lab 4-6	Lab 4-6: Performing Initial Router Configuration		New
5	0	WAN Connections	New	

Module	Lesson	Title	Source	Comments
5	1	Understanding WAN Technologies	INTRO21S07L01.doc	
5	2	Enabling the Internet Connection	INTRO21S07L04.doc	
		DHCP Server	ICND23S03L01.doc	
		NAT and PAT	ICND23S04L03.doc	
		Using Cisco SDM to Configure the Internet Connection (DHCP Client & PAT)	New	
5	3	Enabling Static Routing	ICND23S03L01.doc	
5	Lab 5-1	Lab 5-1: Connecting to the Internet	New	
5	4	Configuring Serial Encapsulation	INTRO21S07L02.doc	
			INTRO21S07L03.doc	
		Frame Relay	INTRO21S07L04.doc	
		Asynchronous Transfer Mode and Cell Switching	INTRO21S07L04.doc	
		HDLC	ICND23S05L02.doc	
		PPP	ICND23S05L02.doc	
5	Lab 5-2	Lab 5-2: Connecting to the Main Office	New	
5	5	Enabling RIP	ICND23S03L01.doc	
5	5	Distance Vector Route Selection	ICND23S03L02.doc	
5	5	RIP Features	ICND23S03L04.doc	
5	Lab 5-3	Lab 5-3: Enabling Dynamic Routing to the Main Office	New	
6	0	Network Environment Management	INTRO21S09L00.doc	
6	1	Discovering Neighbors on the Network	INTRO21S09L01.doc	
6	Lab 6-1	Lab 6-1: Using Cisco Discovery Protocol	New	
6	2	Managing Cisco Router Startup and Configuration	INTRO21S09L03.doc	
6	Lab 6-2	Lab 6-2: Managing Router Startup Options	New	
6	3	Managing Cisco Devices	INTRO21S09L04.doc	
6	Lab 6-3	Lab 6-3: Managing Cisco Devices	New	
6	Lab 6-4	Lab 6-4: Confirming the Reconfiguration of the Branch Network	New	