

Table of Contents

Volume 1

<u>Course Introduction</u>	<u>1</u>
Overview	1
Course Goal and Objectives	1
Course Outline	2
Cisco Certifications	3
Learner Skills and Knowledge	4
Learner Responsibilities	5
General Administration	6
Course Flow	7
Icons and Symbols	8
Learner Introductions	9
Course Evaluations	10
<u>Configuring Catalyst Switch Operations</u>	<u>1-1</u>
Overview	1-1
Outline	1-2
<u>Basic Layer 2 Switching and Bridging Functions</u>	<u>1-3</u>
Overview	1-3
Relevance	1-3
Objectives	1-3
Learner Skills and Knowledge	1-4
Outline	1-4
Functions of Ethernet Switches and Bridges	1-5
Frame Transmission Modes	1-7
How Switches and Bridges Learn Source MAC Addresses	1-9
How Switches and Bridges Forward and Filter Frames	1-12
Summary	1-15
References	1-15
Quiz	1-16
Quiz Answer Key	1-18
<u>Redundant Topology Overview</u>	<u>1-19</u>
Overview	1-19
Relevance	1-19
Objectives	1-19

Learner Skills and Knowledge	1-20
Outline	1-20
Redundant Switched and Bridged Topologies	1-21
Broadcast Storms	1-22
Multiple Frame Transmissions	1-23
MAC Database Instability	1-24
Summary	1-25
References	1-25
Quiz	1-26
Quiz Answer Key	1-28
Spanning Tree Protocol Overview	1-29
Overview	1-29
Relevance	1-29
Objectives	1-29
Learner Skills and Knowledge	1-30
Outline	1-30
Spanning Tree Protocol	1-31
Spanning-Tree Operation	1-32
Selecting the Root Bridge	1-33
Stages of Spanning-Tree Port States	1-34
Spanning-Tree Recalculation	1-39
Rapid Spanning-Tree Protocol	1-41
RSTP Port States	1-42
Summary	1-44
References	1-44
Quiz	1-45
Quiz Answer Key	1-48
Configuring a Catalyst Switch	1-49
Overview	1-49
Relevance	1-49
Objectives	1-49
Learner Skills and Knowledge	1-50
Outline	1-50
Verifying the Catalyst Switch Default Configuration	1-51
Configuring the Catalyst Switch IP Address and Default Gateway	1-54
Duplexing and Speed	1-57
Configuring the Duplex Interface	1-58

Managing the MAC Address Table	1-60
Configuring Static MAC Addresses	1-62
Configuring Port Security	1-64
Executing Adds, Moves, and Changes	1-67
Managing Device Configuration Files	1-70
Summary	1-72
References	1-73
Next Steps	1-73
Quiz	1-74
Quiz Answer Key	1-78
Lesson Assessments	1-79
Overview	1-79
Outline	1-79
Lesson Assessment 1-1: Basic Layer 2 Switching and Bridging Functions	1-80
Objectives	1-80
Quiz	1-80
Scoring	1-81
Lesson Assessment 1-2: Redundant Topology Overview	1-82
Objectives	1-82
Quiz	1-82
Scoring	1-83
Lesson Assessment 1-3: Spanning Tree Protocol Overview	1-84
Objectives	1-84
Quiz	1-84
Scoring	1-86
Lesson Assessment 1-4: Configuring a Catalyst Switch	1-87
Objectives	1-87
Quiz	1-87
Scoring	1-90
Lesson Assessment Answer Key	1-91
<i>Extending Switched Networks with VLANs</i>	2-1
Overview	2-1
Outline	2-2
<i>VLAN Operation Overview</i>	2-3
Overview	2-3
Relevance	2-3

Objectives	2-3
Learner Skills and Knowledge	2-3
Outline	2-4
Defining a VLAN	2-5
VLAN Operation	2-6
VLAN Membership Modes	2-7
802.1Q Trunking	2-8
ISL Protocol and Encapsulation	2-13
VTP Protocol Features	2-15
VTP Modes, Operation, and Pruning	2-16
Summary	2-19
References	2-20
Quiz	2-21
Quiz Answer Key	2-24
Configuring VLANs	2-25
Overview	2-25
Relevance	2-25
Objectives	2-26
Learner Skills and Knowledge	2-26
Outline	2-26
Configuring VTP	2-27
Configuring 802.1Q Trunking	2-30
Configuring ISL Trunking	2-33
Configuring a VLAN	2-34
Assigning Ports to a VLAN	2-37
Verifying the VLAN Configuration	2-38
Executing Adds, Moves, and Changes for VLANs	2-45
Adding VLANs and Port Membership	2-45
Changing VLANs and Port Membership	2-46
Deleting VLANs and Port Membership	2-46
Troubleshooting VLANs	2-47
Summary	2-53
References	2-54
Next Steps	2-54
Quiz	2-55
Quiz Answer Key	2-59

<u>Lesson Assessments</u>	2-61
Overview	2-61
Outline	2-61
Lesson Assessment 2-1: VLAN Operation Overview	2-62
Objectives	2-62
Quiz	2-62
Scoring	2-64
Lesson Assessment 2-2: Configuring VLANs	2-65
Objectives	2-65
Quiz	2-65
Scoring	2-68
Lesson Assessment Answer Key	2-69
<u>Determining IP Routes</u>	3-1
Overview	3-1
Outline	3-2
<u>Routing Overview</u>	3-3
Overview	3-3
Relevance	3-3
Objectives	3-3
Learner Skills and Knowledge	3-4
Outline	3-4
Introducing Routing	3-5
Comparing Static and Dynamic Routes	3-7
Configuring Static Routes	3-8
Configuring Default Route Forwarding	3-11
Verifying the Static Routing Configuration	3-12
Introducing Dynamic Routing Protocols	3-13
Using the ip classless Command	3-20
InterVLAN Routing	3-21
Summary	3-25
References	3-26
Quiz	3-27
Quiz Answer Key	3-30

Distance Vector Routing	3-31
Overview	3-31
Relevance	3-31
Objectives	3-31
Learner Skills and Knowledge	3-31
Outline	3-32
Selecting Distance Vector Routes	3-33
Maintaining Routing Information	3-36
How Routing Inconsistencies Occur with Distance Vector Routing Protocols	3-37
Defining a Maximum to Prevent Count to Infinity	3-41
Solutions to Eliminate Routing Loops	3-43
Distance Vector Operations	3-49
Summary	3-55
References	3-56
Quiz	3-57
Quiz Answer Key	3-59
Link-State and Balanced Hybrid Routing	3-61
Overview	3-61
Relevance	3-61
Objectives	3-61
Learner Skills and Knowledge	3-61
Outline	3-62
How Routing Information Is Maintained with Link State	3-63
Link-State Routing Protocol Algorithms	3-67
Example	3-68
Benefits and Drawbacks of Link-State Routing	3-69
When to Use Link-State Routing Protocols	3-70
Balanced Hybrid Routing	3-73
Summary	3-74
References	3-74
Quiz	3-75
Quiz Answer Key	3-77
Enabling RIP	3-79
Overview	3-79
Relevance	3-79
Objectives	3-79
Learner Skills and Knowledge	3-79

Outline	3-80
RIP Features	3-81
Configuring Dynamic Routing Protocols	3-82
Configuring RIP	3-84
Verifying the RIP Configuration	3-86
Troubleshooting the RIP Configuration	3-88
Summary	3-89
References	3-89
Quiz	3-90
Quiz Answer Key	3-92
Enabling IGRP	3-93
Overview	3-93
Relevance	3-93
Objectives	3-93
Learner Skills and Knowledge	3-93
Outline	3-94
IGRP Features	3-95
IGRP Metrics	3-96
Supporting Multiple Paths with IGRP	3-97
Configuring IGRP	3-98
Verifying the IGRP Configuration	3-101
Troubleshooting the IGRP Configuration	3-103
Summary	3-109
References	3-109
Quiz	3-110
Quiz Answer Key	3-113
Enabling EIGRP	3-115
Overview	3-115
Relevance	3-115
Objectives	3-115
Learner Skills and Knowledge	3-115
Outline	3-116
EIGRP Features	3-117
Comparing EIGRP and IGRP	3-119
Configuring EIGRP Protocol	3-120
Verifying the EIGRP Configuration	3-122

Troubleshooting the EIGRP Configuration	3-123
Summary	3-124
References	3-124
Quiz	3-125
Quiz Answer Key	3-127
Enabling OSPF	3-129
Overview	3-129
Relevance	3-129
Objectives	3-129
Learner Skills and Knowledge	3-129
Outline	3-130
OSPF Features	3-131
Comparing OSPF with Distance Vector Routing Protocols	3-132
Shortest Path Algorithm	3-135
Configuring Single Area OSPF	3-136
Verifying the OSPF Configuration	3-139
Troubleshooting the OSPF Configuration	3-140
Summary	3-142
References	3-143
Quiz	3-144
Quiz Answer Key	3-146
Variable-Length Subnet Masks	3-147
Overview	3-147
Relevance	3-147
Objectives	3-147
Learner Skills and Knowledge	3-147
Outline	3-148
VLSM Features	3-149
Route Summarization with VLSM	3-152
Summary	3-159
References	3-159
Next Steps	3-159
Quiz	3-160
Quiz Answer Key	3-161

Lesson Assessments	3-163
Overview	3-163
Outline	3-163
Lesson Assessment 3-1: Routing Overview	3-164
Objectives	3-164
Quiz	3-164
Scoring	3-167
Lesson Assessment 3-2: Distance Vector Routing	3-168
Objectives	3-168
Quiz	3-168
Scoring	3-170
Lesson Assessment 3-3: Link-State and Balanced Hybrid Routing	3-171
Objectives	3-171
Quiz	3-171
Scoring	3-171
Lesson Assessment 3-4: Enabling RIP	3-172
Objectives	3-172
Quiz	3-172
Scoring	3-173
Lesson Assessment 3-5: Enabling IGRP	3-174
Objectives	3-174
Quiz	3-174
Scoring	3-176
Lesson Assessment 3-6: Enabling EIGRP	3-177
Objectives	3-177
Quiz	3-177
Scoring	3-178
Lesson Assessment 3-7: Enabling OSPF	3-179
Objectives	3-179
Quiz	3-179
Scoring	3-181
Lesson Assessment 3-8: Variable-Length Subnet Masks	3-182
Objectives	3-182
Quiz	3-182
Scoring	3-182
Lesson Assessment Answer Key	3-183

Volume 2

Managing IP Traffic with Access Lists **4-1**

Overview	4-1
Outline	4-1

Access Lists and Their Applications **4-3**

Overview	4-3
Relevance	4-3
Objectives	4-3
Learner Skills and Knowledge	4-4
Outline	4-4
Introducing Access Lists	4-5
Example of Access List Implementation	4-5
Access List Applications	4-6
Types of Access Lists	4-8
How Access Lists Operate	4-12
Testing Against Access List Statements	4-14
Wildcard Masking	4-15
Summary	4-19
References	4-20
Quiz	4-21
Quiz Answer Key	4-24

Configuring IP Access Lists **4-25**

Overview	4-25
Relevance	4-25
Objectives	4-25
Learner Skills and Knowledge	4-26
Outline	4-26
Implementing Access Lists	4-27
Configuring Standard IP Access Lists	4-30
Configuring Extended IP Access Lists	4-35
Using Named Access Lists	4-39
Configuring Virtual Terminal Access Lists	4-40
Guidelines for Placing Access Lists	4-44
Verifying the Access List Configuration	4-46
Summary	4-48
References	4-49

Quiz	4-50
Quiz Answer Key	4-53
<u>Scaling the Network with NAT and PAT</u>	<u>4-55</u>
Overview	4-55
Relevance	4-55
Objectives	4-55
Learner Skills and Knowledge	4-56
Outline	4-56
Introducing NAT and PAT	4-57
Translating Inside Source Addresses	4-60
Overloading an Inside Global Address	4-66
Verifying the NAT and PAT Configuration	4-70
Troubleshooting the NAT and PAT Configuration	4-74
Summary	4-77
References	4-77
Next Steps	4-77
Quiz	4-78
Quiz Answer Key	4-81
<u>Lesson Assessments</u>	<u>4-83</u>
Overview	4-83
Outline	4-83
Lesson Assessment 4-1: Access Lists and Their Applications	4-84
Objectives	4-84
Quiz	4-84
Scoring	4-86
Lesson Assessment 4-2: Configuring IP Access Lists	4-87
Objectives	4-87
Quiz	4-87
Scoring	4-89
Lesson Assessment 4-3: Scaling the Network with NAT and PAT	4-90
Objectives	4-90
Quiz	4-90
Scoring	4-92
Lesson Assessment Answer Key	4-93

<u>Establishing Serial Point-to-Point Connections</u>	<u>5-1</u>
Overview	5-1
Outline	5-1
<u>Wide-Area Networking Review</u>	<u>5-3</u>
Overview	5-3
Relevance	5-3
Objectives	5-3
Learner Skills and Knowledge	5-4
Outline	5-4
WAN Review	5-5
WAN Connection Types	5-6
WAN Cabling	5-8
Layer 2 Encapsulation Protocols	5-10
Summary	5-12
References	5-12
Quiz	5-13
Quiz Answer Key	5-15
<u>Configuring Serial Point-to-Point Encapsulation</u>	<u>5-17</u>
Overview	5-17
Relevance	5-17
Objectives	5-17
Learner Skills and Knowledge	5-18
Outline	5-18
Configuring HDLC Encapsulation	5-19
PPP Layered Architecture	5-21
Configuring PPP	5-23
Establishing a PPP Session	5-24
PPP Authentication Protocols	5-25
Configuring PPP Authentication	5-27
Verifying the Serial Encapsulation Configuration	5-32
Troubleshooting the PPP Authentication Configuration	5-33
Summary	5-34
References	5-35
Next Steps	5-35
Quiz	5-36
Quiz Answer Key	5-39

<u>Lesson Assessments</u>	5-41
Overview	5-41
Outline	5-41
Lesson Assessment 5-1: Wide-Area Networking Review	5-42
Objectives	5-42
Quiz	5-42
Scoring	5-43
Lesson Assessment 5-2: Configuring Serial Point-to-Point Encapsulation	5-44
Objectives	5-44
Quiz	5-44
Scoring	5-46
Lesson Assessment Answer Key	5-47
<u>Establishing Frame Relay Connections</u>	6-1
Overview	6-1
Outline	6-1
<u>Frame Relay Overview</u>	6-3
Overview	6-3
Relevance	6-3
Objectives	6-3
Learner Skills and Knowledge	6-3
Outline	6-4
Introducing Frame Relay	6-5
Frame Relay Stack Layered Support	6-6
Frame Relay Terminology	6-7
Frame Relay Topologies	6-9
Resolving Reachability Issues in Frame Relay	6-10
Frame Relay Address Mapping	6-12
Frame Relay Signaling	6-13
How Service Providers Map Frame Relay Data-Link Connection Identifiers	6-16
Service Provider Frame Relay-to-ATM Interworking	6-18
Summary	6-20
References	6-21
Quiz	6-22
Quiz Answer Key	6-26

Configuring Frame Relay	6-27
Overview	6-27
Relevance	6-27
Objectives	6-27
Learner Skills and Knowledge	6-27
Outline	6-28
Configuring a Basic Frame Relay Network	6-29
Configuring a Static Frame Relay Map	6-31
Configuring Frame Relay Subinterfaces	6-32
Verifying Basic Frame Relay Operations	6-36
Troubleshooting Basic Frame Relay Operations	6-42
Summary	6-45
References	6-45
Next Steps	6-45
Quiz	6-46
Quiz Answer Key	6-49
Lesson Assessments	6-51
Overview	6-51
Outline	6-51
Lesson Assessment 6-1: Frame Relay Overview	6-52
Objectives	6-52
Instructions	6-52
Scoring	6-55
Lesson Assessment 6-2: Configuring Frame Relay	6-56
Objectives	6-56
Instructions	6-56
Scoring	6-58
Lesson Assessment Answer Key	6-59
Completing ISDN Calls	7-1
Overview	7-1
Outline	7-1
Completing ISDN Calls	7-1
Overview	7-1
Outline	7-1

Configuring ISDN BRI and PRI **7-3**

Overview	7-3
Relevance	7-3
Objectives	7-3
Learner Skills and Knowledge	7-3
Outline	7-4
Introducing ISDN	7-5
ISDN Standards and Access Methods	7-6
Establishing an ISDN BRI or PRI Call	7-8
ISDN Functions and Reference Points	7-9
Determining the Router ISDN Interface	7-11
ISDN Switch Types	7-14
Configuring ISDN BRI	7-16
Configuring ISDN PRI	7-18
Verifying the ISDN Configuration	7-21
Troubleshooting the ISDN Configuration	7-22
Summary	7-23
References	7-24
Quiz	7-25
Quiz Answer Key	7-29

Configuring Dial-on-Demand Routing **7-31**

Overview	7-31
Relevance	7-31
Objectives	7-31
Learner Skills and Knowledge	7-32
Outline	7-32
Introducing DDR	7-33
DDR Operation	7-35
Configuring Legacy DDR	7-36
Defining Static Routes for DDR	7-37
Specifying Interesting Traffic for DDR	7-39
Configuring DDR Dialer Information	7-41
Configuring ISDN PRI and Legacy DDR	7-46
Verifying the DDR Configuration	7-51
Troubleshooting the DDR Configuration	7-53
Troubleshooting Inbound Calls	7-56

Troubleshooting Outbound Calls	7-57
Summary	7-59
References	7-60
Next Steps	7-60
Quiz	7-61
Quiz Answer Key	7-65
Lesson Assessments	7-67
Overview	7-67
Outline	7-67
Lesson Assessment 7-1: Configuring ISDN BRI and PRI	7-68
Objectives	7-68
Quiz	7-68
Scoring	7-71
Lesson Assessment 7-2: Configuring Dial-on-Demand Routing	7-72
Objectives	7-72
Quiz	7-72
Scoring	7-75
Lesson Assessment Answer Key	7-76
<u>Course Glossary</u>	<u>1</u>

Course Introduction

Overview

Interconnecting Cisco Network Devices (ICND) v2.1 is an instructor-led course presented by Cisco Systems training partners to their end-user customers. This five-day course focuses on using Cisco Catalyst switches and Cisco routers connected in LANs and WANs that are typically found at small to medium network sites.

Upon completion of this training course, you will be able to configure, verify, and troubleshoot the various Cisco networking devices.

Course Goal and Objectives

This section describes the course goal and objectives.

Course Goal

Cisco.com

“To implement and operate a simple Cisco network that includes switches, routers, and remote access routers”

Interconnecting Cisco Network Devices

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—0-4

Upon completing this course, you will be able to meet these objectives:

- Explain how bridging and switching operate
- Explain the purpose and operation of the Spanning Tree Protocol
- Build a functional router configuration to support specified network operational requirements, given a network design
- Describe the features and operation of static routing
- Build a functional configuration to support specified network operational requirements, given a network design
- Use the appropriate **show** commands to display network operational parameters so that anomalies are detected
- Use the appropriate **debug** commands to monitor network operational parameters so that events and anomalies are detected

Course Outline

This outline lists the modules included in this course.

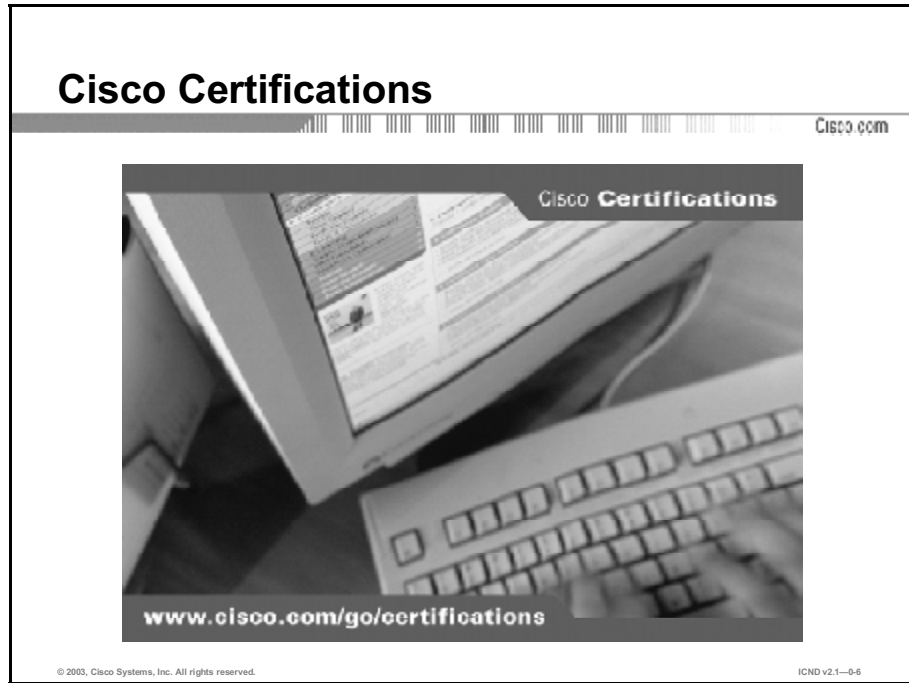
Course Outline

- **Configuring Catalyst Switch Operations**
- **Extending Switched Networks with VLANs**
- **Determining IP Routes**
- **Managing IP Traffic with Access Lists**
- **Establishing Serial Point-to-Point Connections**
- **Establishing Frame Relay Connections**
- **Completing ISDN Calls**

© 2003, Cisco Systems, Inc. All rights reserved.Cisco.comICND v2.1—0-5

Cisco Certifications

This topic lists the certification requirements of this course.

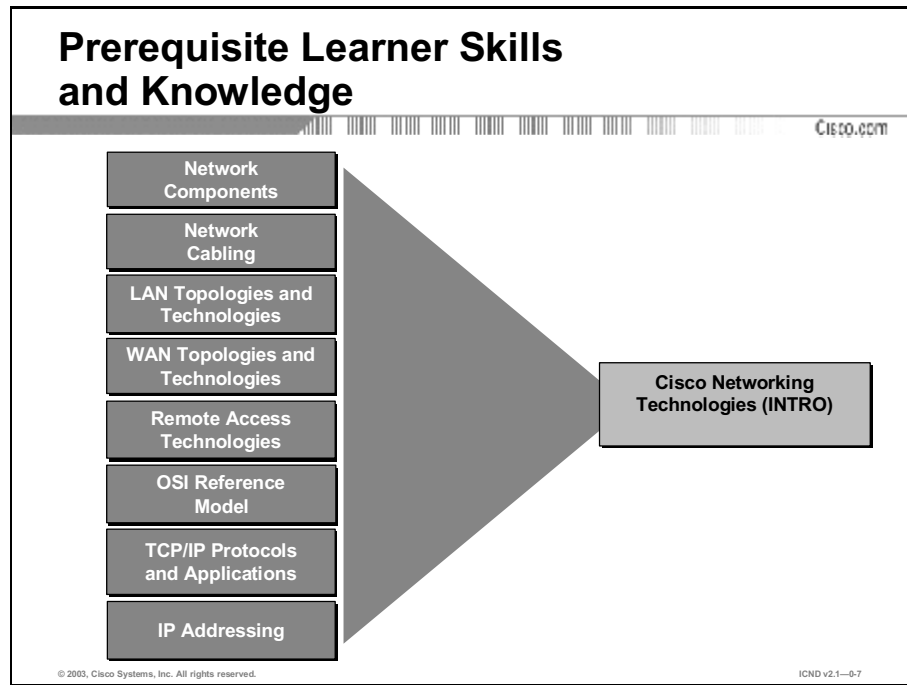


Cisco provides three levels of general career certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused Cisco Qualified Specialist (CQS) certifications for designated areas such as cable communications, voice, and security.

There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to <http://www.cisco.com/go/certifications>.

Learner Skills and Knowledge

This topic lists the course prerequisites.



To benefit fully from this lesson, you must have the prerequisite skills and knowledge listed in the figure.

Learner Responsibilities

This topic discusses the responsibilities of the learners.

Learner Responsibilities



- **Complete prerequisites**
- **Introduce yourself**
- **Ask questions**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—0-8

To take full advantage of the information presented in this course, you must have completed the prerequisite requirements.

In class, you are expected to participate in all lesson exercises and assessments.

In addition, you are encouraged to ask any questions relevant to the course materials.

If you have pertinent information or questions concerning future Cisco product releases and product features, please discuss these topics during breaks or after class. The instructor will answer your questions or direct you to an appropriate information source.

General Administration

This topic lists the administrative issues for the course.

General Administration

Cisco.com

Class-Related	Facilities-Related
• Sign-in sheet • Course materials • Length and times • Attire	• Site emergency procedures • Rest rooms • Telephones/faxes • Break and lunchroom locations

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—0-9

The instructor will discuss the administrative issues noted here so that you know exactly what to expect from the class.

- Sign-in process
- Starting and anticipated ending times of each class day
- Class breaks and lunch facilities
- Appropriate attire during class
- Materials that you can expect to receive during class
- What to do in the event of an emergency
- Location of the rest rooms
- How to send and receive telephone and fax messages

Course Flow

This topic covers the suggested flow of the course materials.

Course Flow

Cisco.com

A
M

Day 1	Day 2	Day 3	Day 4	Day 5
Course Introduction	Module 2: Extending Switched Networks with VLANs (Cont.)	Module 3: Determining IP Routes (Cont.)	Module 4: Managing IP Traffic with Access Lists	Module 6: Establishing Frame Relay Connections
Module 1: Configuring Catalyst Switch Operations	Module 3: Determining IP Routes			

Lunch

P
M

Module 1: Configuring Catalyst Switch Operations (Cont.)	Module 3: Determining IP Routes (Cont.)	Module 3: Determining IP Routes (Cont.)	Module 4: Managing IP Traffic with Access Lists (Cont.)	Module 7: Completing ISDN Calls
Module 2: Extending Switched Networks with VLANs			Module 5: Establishing Serial Point-to-Point Connections	

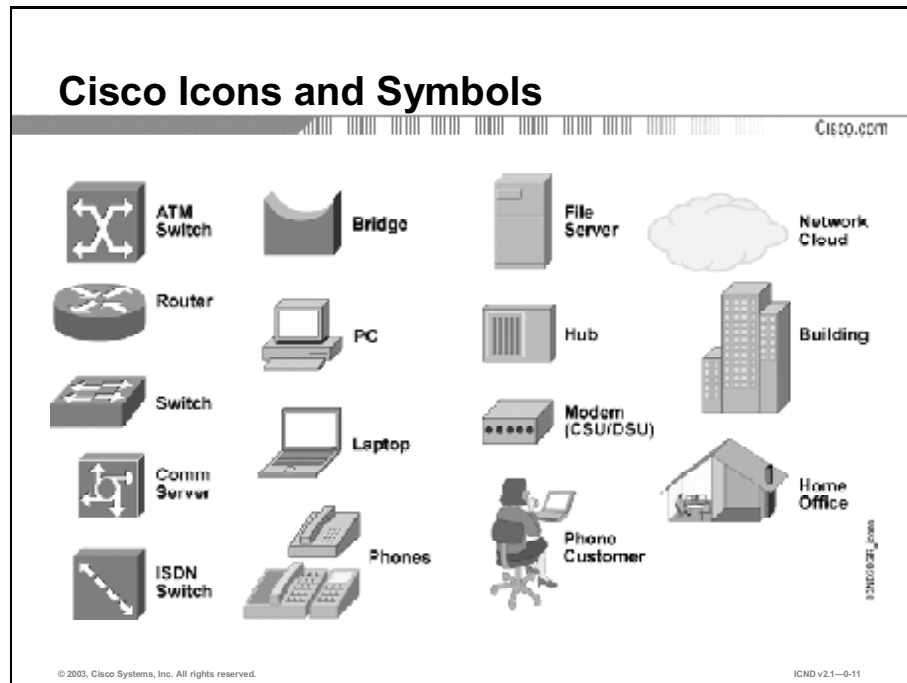
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—0-10

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the laboratory exercises. The exact timing of the subject materials and labs depends on the pace of your specific class.

Icons and Symbols

This topic shows the Cisco icons and symbols that are used in this course.



Learner Introductions

This is the point in the course where you introduce yourself.

Learner Introductions

Cisco.com

- **Your name**
- **Your company**
- **Skills and knowledge**
- **Brief history**
- **Objective**



© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—0-12

Prepare to share the following information:

- Your name
- Your company
- If you have most or all of the prerequisite skills
- A profile of your experience
- What you would like to learn from this course

Course Evaluations

Cisco relies on customer feedback to make improvements and guide business decisions. Your valuable input will help shape future Cisco learning products and program offerings.



On the first and final days of class, your instructor will provide the following information needed to fill out the evaluation:

- Course acronym (*printed on student kit side label*) _____
- Course version number (*printed on student kit side label*) _____
- Cisco Learning Partner ID # _____
- Instructor ID # _____
- Course ID # (*for courses registered in Cisco Learning Locator*) _____

Please use this information to complete a brief (approximately 10 minutes) online evaluation concerning your instructor and the course materials in the student kit. To access the evaluation, go to <http://www.cisco.com/go/clpevals>.

After the completed survey has been submitted, you will be able to access links to a variety of Cisco resources, including information on the Cisco Career Certification programs and future Cisco Networkers events.

If you encounter any difficulties accessing the course evaluation URL or submitting your evaluation, please contact Cisco via email at clpevals_support@external.cisco.com.

Configuring Catalyst Switch Operations

Overview

The Cisco Catalyst 1900 series switches and the Cisco Catalyst 2950 series switches are designed for plug-and-play operation: you need only to assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can configure and monitor the switch on an individual basis or as part of a switch cluster through its various management interfaces. This module shows you how to configure a Catalyst switch for basic operations.

Upon completing this module, you will be able to:

- Explain how bridging and switching operates
- Explain the purpose and operations of the Spanning Tree Protocol
- Verify the default configuration of the device, given a functioning access layer switch
- Build a functional access switch configuration to support the specified network operational parameters, given a network design
- Execute an add, move, or change on an access layer switch, given a new network requirement

Outline

The module contains these lessons:

- Basic Layer 2 Switching and Bridging Functions
- Redundant Topology Overview
- Spanning Tree Protocol Overview
- Configuring a Catalyst Switch
- Lesson Assessments

Basic Layer 2 Switching and Bridging Functions

Overview

Layer 2 LAN switches and bridges operate at Layer 2 of the Open System Interconnection (OSI) reference model, while hubs operate at Layer 1. Operating at Layer 2 offers more intelligence for making forwarding decisions. LAN switches and bridges are more intelligent than hubs because they can actually listen in on the traffic going through to examine the source and destination MAC addresses, and they can build a MAC address table that enables them to make intelligent forwarding decisions at Layer 2. This lesson explains the basic functions provided by LAN switches and bridges.

Relevance

You should be familiar with general LAN switching and bridging functions before configuring a Catalyst switch.

Objectives

Upon completing this lesson, you will be able to:

- Describe Layer 2 switching and bridging operations and modes
- Describe how LAN switches use and populate the MAC address table

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

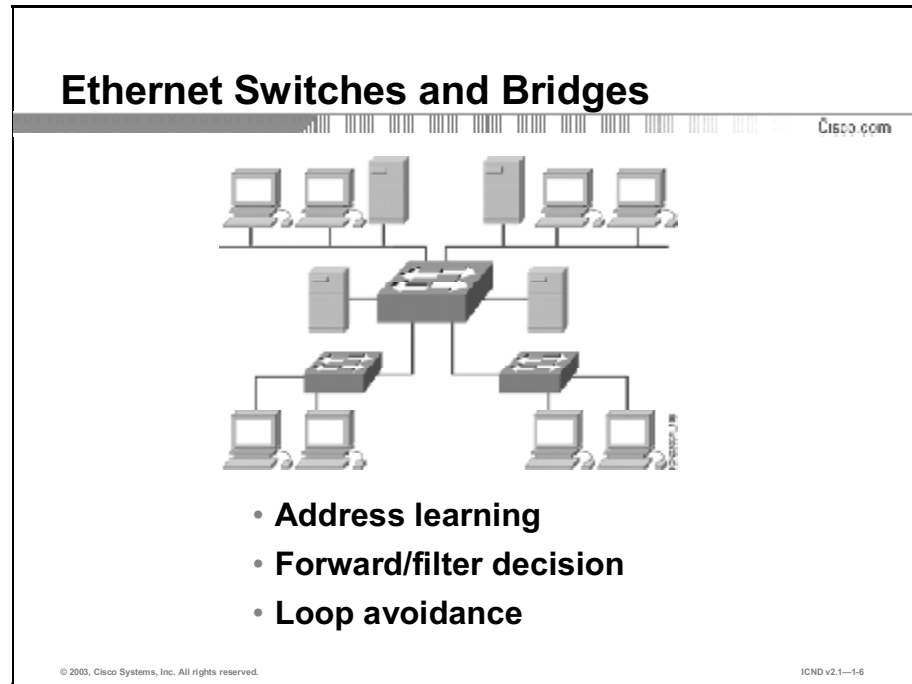
Outline

The lesson includes these topics:

- Overview
- Functions of Ethernet Switches and Bridges
- Frame Transmission Modes
- How Switches and Bridges Learn Source MAC Addresses
- How Switches and Bridges Forward and Filter Frames
- Summary
- Quiz

Functions of Ethernet Switches and Bridges

Ethernet switches and bridges increase the available bandwidth by reducing the number of devices contending for the segment bandwidth. Ethernet switches and bridges also make intelligent frame-forwarding decisions by examining the source and destination MAC address of incoming frames. This topic describes the basic functions of Ethernet switches and bridges.



Ethernet switches and bridges operate at Layer 2 of the Open System Interconnection (OSI) reference model. Because of their high-speed internal architecture and high number of ports, Ethernet switches offer much higher throughput than a traditional bridge.

Switches and bridges perform the following functions:

- An Ethernet switch or bridge learns the MAC addresses of the devices that are attached to each of its ports. They do this by listening in on the incoming traffic to examine the source MAC addresses of the incoming frames on its ports. The MAC address-to-port mappings are stored in a MAC database. This MAC database is often called the MAC address table or the content-addressable memory (CAM) table.
- When an Ethernet switch or bridge receives a frame, it consults the MAC database to determine which port can reach the station identified as the destination in the frame. If the destination MAC address is found in the MAC database, the frame is transmitted on only that port. If the destination MAC address is not found in the MAC database, the frame is transmitted out on all ports except the incoming port.

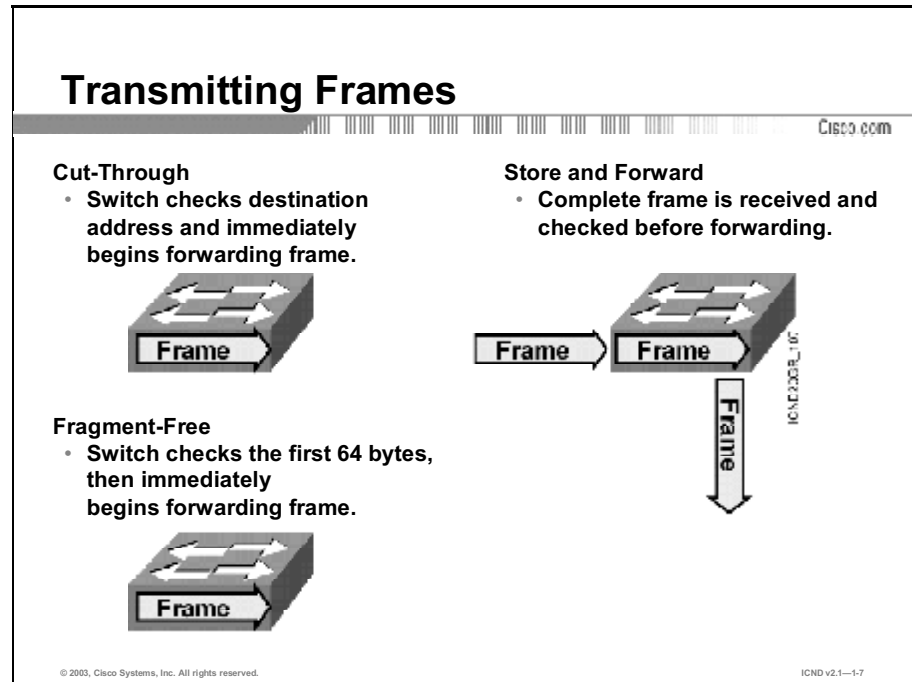
Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in switched or bridged networks.

Bridges became commercially available in the early 1980s. At the time of their introduction, bridges connected and enabled packet forwarding between homogeneous networks. More recently, bridging between different networks has also been defined and standardized.

Today, switching technology has emerged as the evolutionary heir to bridging-based internetworking solutions. Switching implementations now dominate applications in which bridging technologies were implemented in prior network designs. Superior throughput performance, higher port density, lower per-port cost, and greater flexibility have contributed to the emergence of switches as replacement technology for bridges and as complements to routing technology.

Frame Transmission Modes

LAN switches and bridges use one of three operating modes to transmit frames: store and forward, cut-through, and fragment-free. This topic describes the three primary LAN switch and bridge frame transmission modes.



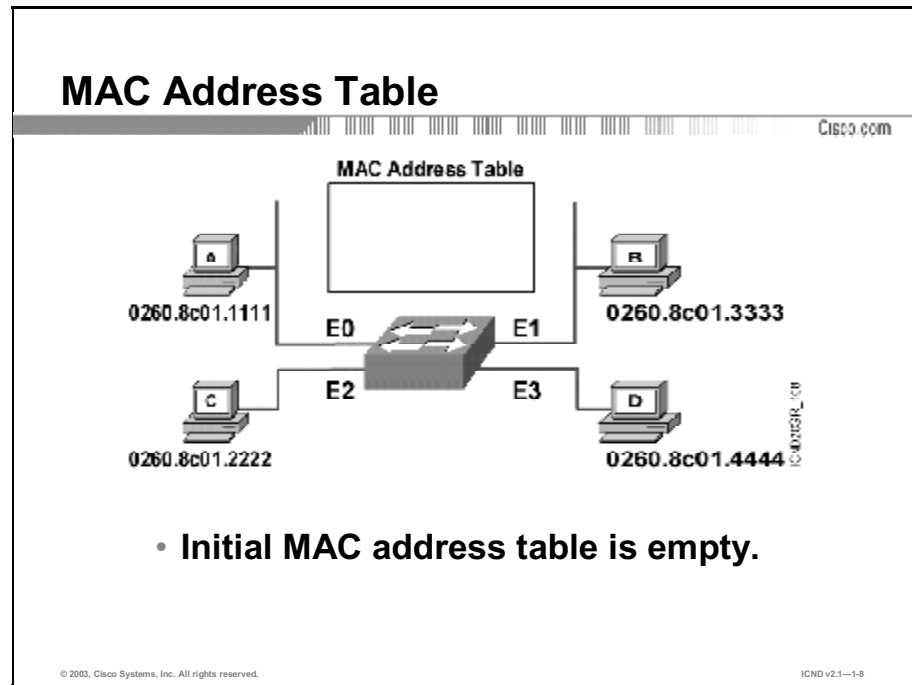
There are three primary operating modes that are used to handle frame switching: store and forward, cut-through, and fragment-free (modified cut-through). Fragment-free is the default switching method on the Cisco Catalyst 1900 series switch, while the Catalyst 2950 series switch uses store and forward.

- **Store and forward:** In the store and forward mode, the switch or bridge receives the complete frame and then forwards it. The destination and source addresses are read, the cyclic redundancy check (CRC) is performed, the relevant filters are applied, and the frame is forwarded. If the CRC is bad, the frame is discarded. Latency through the switch or bridge varies with frame length.
- **Cut-through:** In the cut-through mode, the switch or bridge checks the destination address (DA) as soon as the header is received and immediately begins forwarding the frame. There is a significant decrease in latency compared to the store and forward mode. The delay in cut-through switching remains constant regardless of frame size because this switching mode starts to forward the frame as soon as the switch or bridge reads the destination addresses. In some switches and bridges just the destination addresses are read. Some switches and bridges continue to read the CRC, and keep a count of errors. Although the switch or bridge will not stop an errored frame, if the error rate is too high, the switch or bridge can be set, either manually or automatically, to use the store and forward mode instead. This is often known as *adaptive cut-through*. It combines the low-latency advantage of cut-through and the error protection offered by store and forward.

- **Fragment-free:** In the fragment-free mode, the switch or bridge will read the first 64 bytes (the minimum Ethernet frame size) before forwarding the frame. Usually, collisions happen within the first 64 bytes of a frame. When a collision occurs, a fragment (a frame less than 64 bytes) is created. By reading 64 bytes, the switch or bridge can filter out collision (fragment) frames. Fragment-free has higher latency than cut-through; however, fragment-free can detect fragment frames and discard them rather than forwarding them, in contrast to cut-through, which will forward fragment frames if the destination address exists.

How Switches and Bridges Learn Source MAC Addresses

LAN switches and bridges maintain a MAC address table to store MAC address-to-port mappings so that it can determine the locations of connected devices. This topic describes how a LAN switch or bridge associates a MAC address with a port.



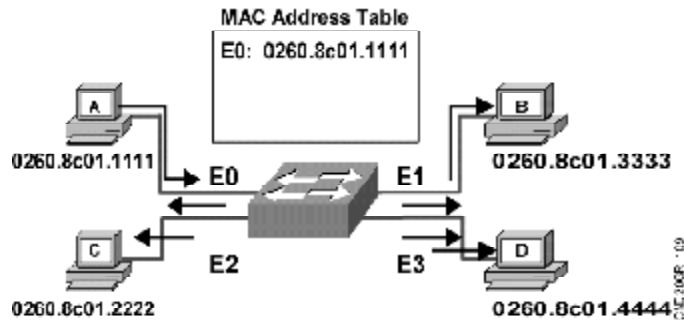
A switch or bridge maintains a MAC address table to track the locations of devices that are connected to the switch or bridge. The size of the MAC address table varies depending on the switch or bridge. For example, the Catalyst 1900 series access layer switch has a MAC address table that can hold up to 1024 entries, while the Catalyst 2950 series can store 8192 entries.

When a switch or bridge is first initialized, the MAC address table is empty. With an empty MAC address table, the switch or bridge must forward each frame to all connected ports other than that on which it arrived. Forwarding a frame to all connected ports except the incoming port is called “flooding” the frame. Flooding is the least efficient way to transmit data across a switch or bridge because it wastes bandwidth.

Switches and bridges implement buffering memory so that they can receive and transmit frames independently on each port.

Learning Addresses

Cisco.com



- Station A sends a frame to station C.
- Switch caches the MAC address of station A to port E0 by learning the source address of data frames.
- The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded).

© 2003, Cisco Systems, Inc. All rights reserved.

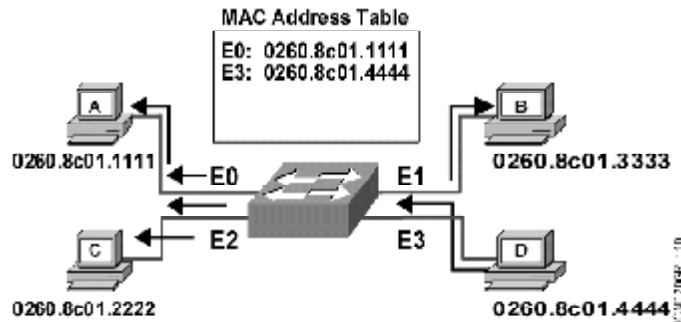
ICND v2.1—1-9

In the example, station A with MAC address 0260.8c01.1111 wants to send traffic to station C with MAC address 0260.8c01.2222. The switch receives this frame and performs several actions, as follows:

- The frame is received from the physical Ethernet 0 port and stored in temporary buffer space, assuming store and forward frame transmission.
- Because the switch does not yet know what interface connects it to the destination station, it will flood the frame through all other ports.
- While flooding the frame from station A, the switch notes the source address of the frame, and associates it with port E0 in a new MAC address table entry.
- A MAC address table entry is created, which stays in the MAC address table up to the age time. If station A does not transmit another frame to the switch before age time expires, that entry will not be refreshed and will be removed from the MAC address table. For example, on the Catalyst 1900 series switch, the age time is set to 5 minutes by default. Because the MAC address table has a limited size, the age time helps to limit flooding by remembering the most active stations in the network. The age time also accommodates station moves. Aging allows the switch or bridge to forget an entry about a station that has been removed. If a station is moved from one port to another port, the switch or bridge will immediately learn the new location of the station as soon as that station begins to transmit frames to the switch or bridge on the new port.

Learning Addresses (Cont.)

Cisco.com



- Station D sends a frame to station C.
- Switch caches the MAC address of station D to port E3 by learning the source address of data frames.
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded).

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-10

The learning process continues when each station sends frames to the others.

Here station D with MAC address 0260.8c01.4444 sends traffic to station C with MAC address 0260.8c01.2222. The switch performs several actions, as follows:

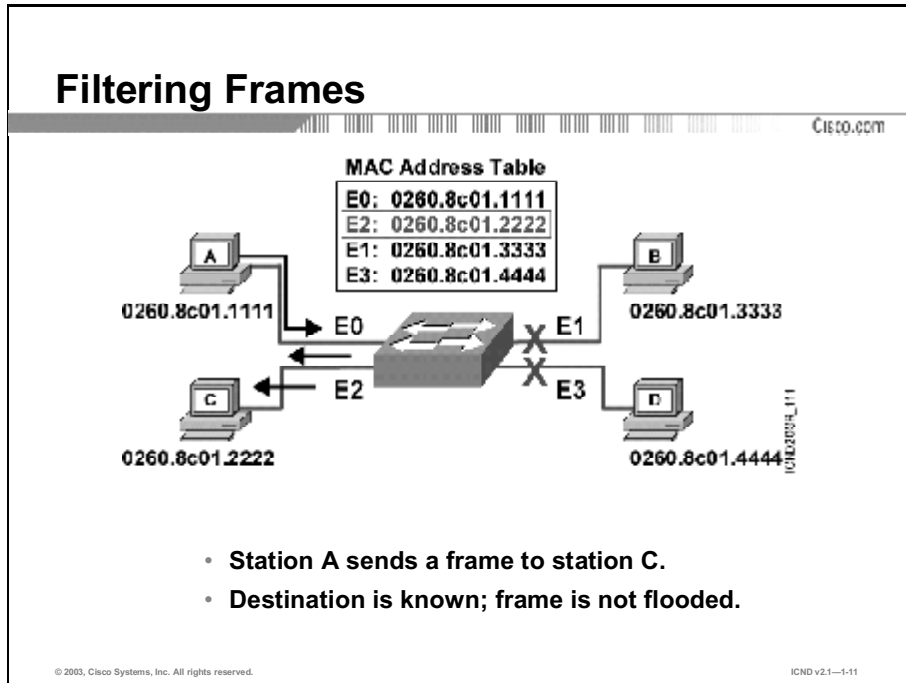
- The source address, 0260.8c01.4444, is added to the MAC address table.
- The destination address from the transmitted frame, station C, is compared with entries in the MAC address table.
- When the switch or bridge determines that no port-to-MAC address mapping yet exists for this destination, the frame is flooded to all ports other than that on which it arrived.

When station C sends a frame back to station A, the switch can also learn the station C MAC address at port E2.

As long as all stations send data frames within the MAC address table entry lifetime, a complete MAC address table is built. These entries are then used to make intelligent Layer 2 forwarding and filtering decisions.

How Switches and Bridges Forward and Filter Frames

When a frame arrives with a known destination address, it is forwarded only on the specific port connected to the destination station. This topic describes how switches and bridges determine where to forward incoming frames.

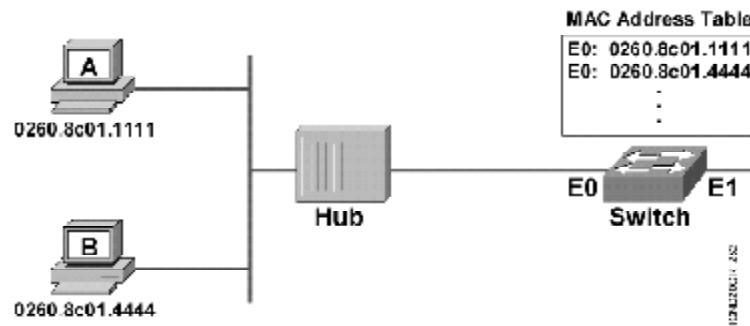


In the figure, station A sends a frame to station C. When the destination station C MAC address exists in the MAC address table, the switch transmits the frame only on the port listed. The sequence is as follows:

- The destination MAC address from the transmitted frame, 0260.8c01.2222, is compared with entries in the MAC address table.
- When the switch or bridge determines that the destination MAC address can be reached through port E2, it transmits the frame to port E2 only.
- The switch does not transmit the frame on ports E1 or E3 to preserve bandwidth on these links. This action is known as frame filtering.
- The switch refreshes the MAC address table entry for the source MAC address.

Filtering Frames (Cont.)

Cisco.com



- Station A sends a frame to station B.
- The switch has the address for station B in the MAC address table.

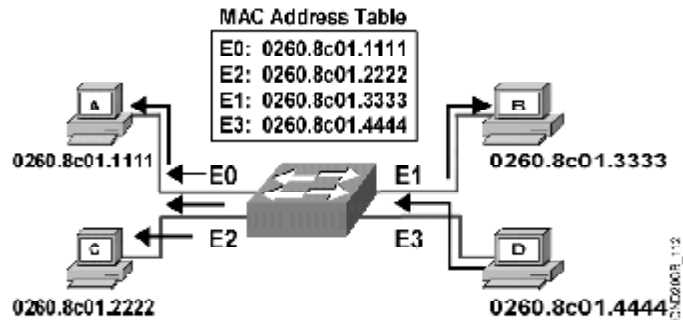
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-12

The figure shows station A and station B connected to the same switch port through a hub. In this case, station A is sending a frame to station B. The switch has learned the addresses of station A and B. The switch will not forward the frame from station A to any ports.

Broadcast and Multicast Frames

Cisco.com



- Station D sends a broadcast or multicast frame.
- Broadcast and multicast frames are flooded to all ports other than the originating port.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-13

Broadcast and multicast frames constitute a special case. Because broadcast and multicast frames may be of interest to all stations, the switch or bridge normally floods broadcast and multicast to all ports other than the originating port. A switch or bridge never learns a broadcast or multicast address because broadcast and multicast addresses never appear as the source address of a frame.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **Ethernet switches and bridges increase the available bandwidth of a network by creating dedicated network segments and interconnecting the segments.**
- **Switches and bridges use one of three operating modes to transmit frames: store and forward, cut-through, and fragment-free.**
- **Switches and bridges maintain a MAC address table to store address-to-port mappings so it can determine the locations of connected devices.**
- **When a frame arrives with a known destination address, it is forwarded only on the specific port connected to the destination station.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-14

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) At what layer of the OSI reference model do LAN switches and bridges operate?
- A) network
 - B) transport
 - C) data-link
 - D) application
- Q2) Which two functions does the MAC database offer? (Choose two.)
- A) offers loop avoidance
 - B) used for making frame-forwarding and filtering decisions
 - C) determines the destination MAC address of each packet it processes
 - D) stores MAC addresses of devices attached to each of the ports on the switch or bridge
 - E) used by the Spanning Tree Protocol to maintain redundant paths in the switched or bridged network
- Q3) Which frame transmission mode reads the entire frame before forwarding it?
- A) cut-through
 - B) fragment-free
 - C) store and forward
 - D) All modes read the entire frame before forwarding it.
- Q4) The cut-through transmission mode forwards a frame immediately after reading ____.
- A) the entire frame
 - B) the destination address
 - C) the contents of the frame
 - D) the first 32 bytes of the frame
 - E) the first 64 bytes of the frame
- Q5) Flooding occurs on a switched or bridged network when ____.
- A) a frame arrives with a source address that is in the MAC address database
 - B) a frame arrives with a source address that is not in the MAC address database
 - C) a frame arrives with a destination address that is in the MAC address database
 - D) a frame arrives with a destination address that is not in the MAC address database

- Q6) What information in a frame does a switch or bridge use to populate the MAC address table?
- A) source ports
 - B) source addresses
 - C) destination ports
 - D) destination addresses
- Q7) Assume station A sends a frame to station B. What will a switch or bridge do to forward the frame to the correct location?
- A) forward the frame to all ports on the switch or bridge
 - B) look up the station A address in its MAC address table and, if it is there, forward the frame out the associated port
 - C) look up the station B address in its MAC address table and, if it is there, forward the frame out the associated port
 - D) look up the station A and station B address in its MAC address table and, if both are there, forward the frame out the associated port
- Q8) Assume station A sends a broadcast frame to a switch. What will the switch do to forward the frame to the correct location?
- A) forward the frame to all ports on the switch or bridge
 - B) forward the frame to all ports except the originating port
 - C) look up the station A address in the MAC address table and, if it is there, forward the frame to the associated port
 - D) look up the broadcast address in the MAC address table and, if it is there, forward the frame to the associated port

Quiz Answer Key

Q1) C

Relates to: Functions of Ethernet Switches and Bridges

Q2) B, D

Relates to: Functions of Ethernet Switches and Bridges

Q3) C

Relates to: Frame Transmission Modes

Q4) B

Relates to: Frame Transmission Modes

Q5) D

Relates to: How Switches and Bridges Learn Source MAC Addresses

Q6) B

Relates to: How Switches and Bridges Learn Source MAC Addresses

Q7) C

Relates to: How Switches and Bridges Forward and Filter Frames

Q8) B

Relates to: How Switches and Bridges Forward and Filter Frames

Redundant Topology Overview

Overview

Most complex networks include redundant devices to avoid single points of failure. While a redundant topology eliminates some problems, it can introduce others. This lesson describes the problems that can be caused by using a redundant topology in a switched or bridged network.

Relevance

You will need to know what problems can arise from a redundant topology so that you can recognize them when they occur.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features of redundant switch and bridge topologies
- Explain the problems associated with broadcast storms, multiple frame transmissions, and MAC address table instability
- Describe loop avoidance and explain how it can solve redundant switch topology issues

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

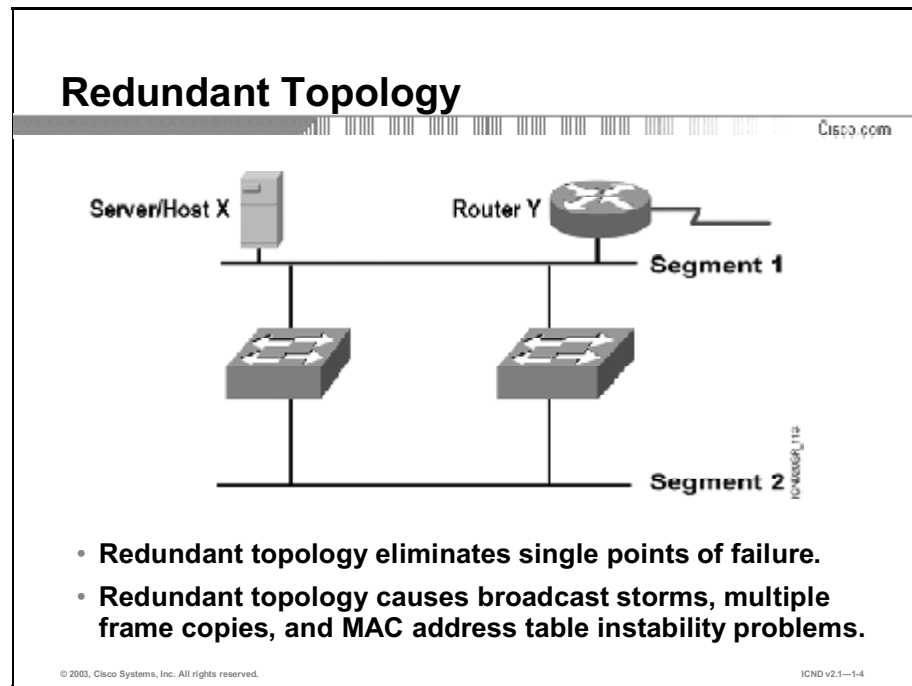
Outline

The lesson includes these topics:

- Overview
- Redundant Switched and Bridged Topologies
- Broadcast Storms
- Multiple Frame Transmissions
- MAC Database Instability
- Summary
- Quiz

Redundant Switched and Bridged Topologies

Bridged and switched networks are commonly designed with redundant links and devices, which can introduce problems, such as broadcast storms, multiple frame transmission, and MAC database instability. This topic describes problems with redundant links and devices in switched or bridged networks.



Redundant links and devices eliminate the possibility that a single point of failure will result in loss of function for the entire switched or bridged network.

While redundant designs may eliminate the single point of failure problem, they introduce several other problems that must be taken into account, as follows:

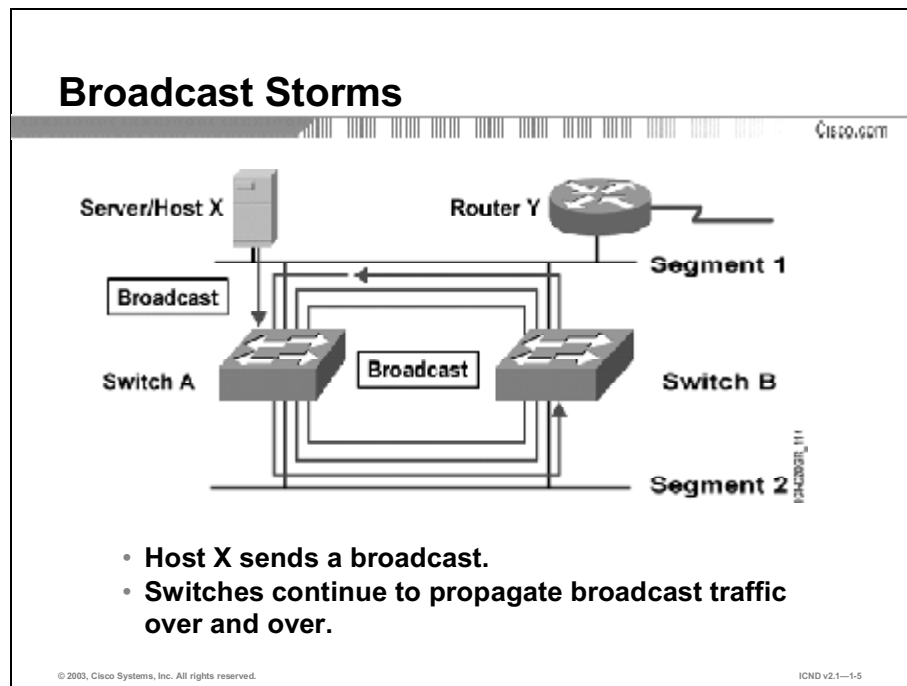
- Without some loop avoidance process in operation, each switch will flood broadcasts endlessly. This situation is commonly called a broadcast storm.
- Multiple copies of unicast frames may be delivered to destination stations. Many protocols expect to receive only a single copy of each transmission. Multiple copies of the same frame may cause unrecoverable errors.
- Instability in the MAC address table content results from copies of the same frame being received on different ports of the switch. Data forwarding may be impaired when the switch consumes the resources that are coping with instability in the MAC address table.

Layer 2 LAN protocols, such as Ethernet, lack a mechanism to recognize and eliminate endlessly looping frames. Some Layer 3 protocols implement a Time to Live (TTL) mechanism that limits the number of times a packet can be retransmitted by a Layer 3 networking device. Lacking such a mechanism, Layer 2 devices will continue to retransmit looping traffic indefinitely.

A loop avoidance mechanism is required to solve each of these problems.

Broadcast Storms

A broadcast storm is when each switch on a redundant network floods broadcast frames endlessly. This topic describes how broadcast storms are created.



Switches flood broadcast frames to all ports except the one on which the frame was received.

The problem of a broadcast storm, as illustrated in the diagram, occurs as follows:

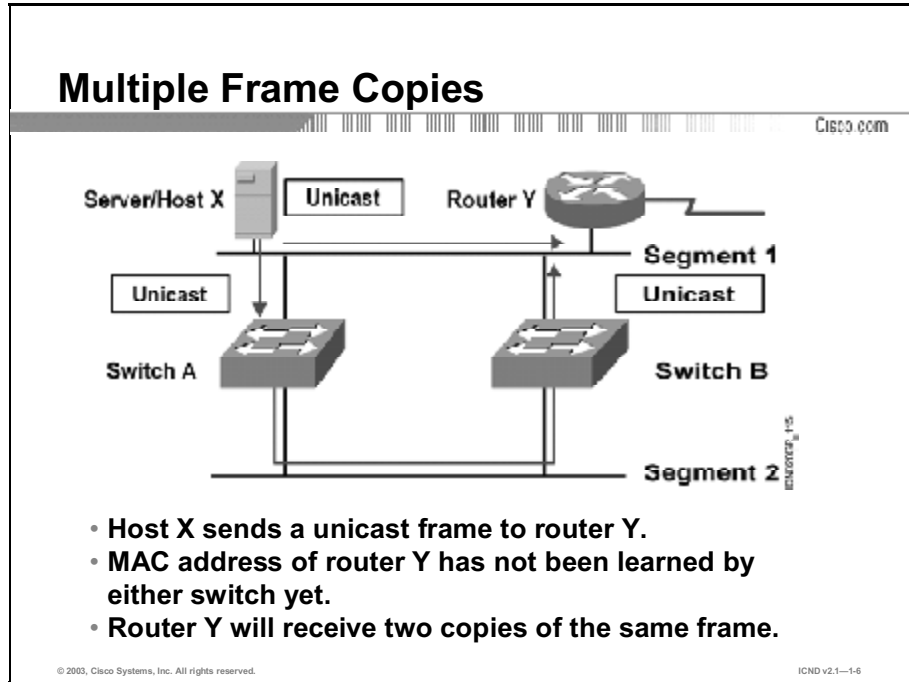
- When host X sends a broadcast frame, such as an Address Resolution Protocol (ARP) for its default gateway (router Y), the frame will be received by switch A.
- Switch A examines the destination address field in the frame and determines that the frame must be flooded onto the bottom Ethernet link, segment 2.
- When this copy of the frame arrives at switch B, the process repeats and a copy of the frame is transmitted onto the top Ethernet, segment 1 near switch B.
- Because the original copy of the frame also arrives at switch B via the top Ethernet, these frames travel around the loop in both directions, even after the destination station has received a copy of the frame.

Broadcast storms can disrupt normal traffic flow. It can also disrupt all the devices on the switched or bridged network because broadcasts must be processed by the CPU in all devices on the segment. For example, it can lock up the user PCs and servers trying to process all of the broadcast frames.

A loop avoidance solution would eliminate this problem by logically breaking the loop, by preventing one of the four interfaces from transmitting frames during normal operation.

Multiple Frame Transmissions

In a redundant topology, multiple copies of the same frame can arrive at the intended host, potentially causing problems with the receiving protocol. This topic explains how multiple frame transmissions occur and the problems that can result.



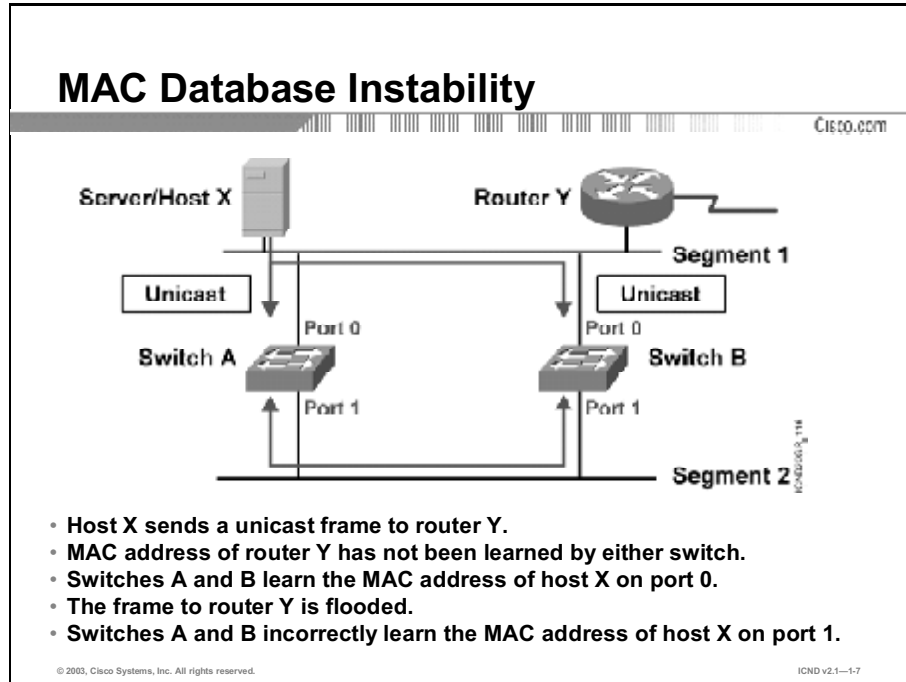
Most protocols are designed *not* to recognize or cope with duplicate transmissions. In general, protocols that make use of a sequence numbering mechanism will assume that many transmissions have failed and that the sequence number has recycled. Other protocols attempt to hand the duplicate transmission to the appropriate upper-layer protocol, with unpredictable results. To see how multiple transmissions can occur, consider the following:

- When host X sends a unicast frame to router Y, one copy is received over the direct Ethernet connection, segment 1, while at more or less the same time, switch A receives a copy and puts it into its buffers.
- If switch A examines the destination address field in the frame and finds no entry in the MAC address table for router Y, switch A floods the frame on all ports except the originating port.
- When switch B receives a copy of the frame through switch A on segment 2, switch B also forwards a copy of the frame onto segment 1 if there is no entry in the MAC address table for router Y.
- Router Y receives a copy of the same frame for the second time.

A loop avoidance solution would eliminate this problem by logically breaking the loop, by preventing one of the four interfaces from transmitting frames during normal operation.

MAC Database Instability

MAC database instability results when multiple copies of a frame arrive on different ports of a switch. This topic describes how MAC database instability can arise and the problems that can result.



In the diagram, switch B installs a mapping between the MAC address of host X and port 0 which connects to segment 1 when the first frame arrives. Sometime later, when the copy of the frame transmitted through switch A arrives at port 1 of switch B, switch B must remove the first entry and install one that incorrectly maps the MAC address of station X to the port 1 which connects to segment 2.

Depending on the internal architecture of the switch in question, it may or may not cope well with rapid changes in its MAC database.

In this instance also, a loop-avoidance solution would eliminate this problem by logically breaking the loop, by preventing one of the four interfaces from transmitting frames during normal operation.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **Bridged and switched networks are commonly designed with redundant links and devices, which can introduce problems, such as broadcast storms, multiple frame transmission, and MAC database instability.**
- **A broadcast storm is when each switch on a redundant network floods broadcast frames endlessly.**
- **In a redundant topology, multiple copies of the same frame can arrive at the intended host, potentially causing problems with the receiving protocol.**
- **MAC database instability results when multiple copies of a frame arrive on different ports of a switch.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-8

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which two problems are associated with redundant switched designs? (Choose two.)
- A) multicast floods
 - B) broadcast storms
 - C) a single copy of multiple frames delivered to a destination station
 - D) a single copy of a frame delivered to multiple destination stations
 - E) multiple copies of a single frame delivered to a destination station
- Q2) Instability in the MAC address table content results from ____.
- A) different frames being received on a single port of the switch
 - B) different frames being received on different ports of the switch
 - C) multiple copies of the same frame being received on the same port of the switch
 - D) multiple copies of the same frame being received on different ports of the switch
- Q3) Which mechanism can you use to eliminate broadcast storms?
- A) loop feedback
 - B) storm aversion
 - C) loop avoidance
 - D) storm prevention
- Q4) Which description applies to a broadcast storm?
- A) A switch receives a broadcast frame, forwards it, receives it again from another switch, forwards it again, and so on indefinitely.
 - B) A switch forwards a broadcast frame to another switch, which forwards the same frame to a third switch, which forwards it to a fourth switch, and so on indefinitely.
 - C) A switch receives a broadcast frame, forwards it, receives it again from another switch, forwards it again, and so on until the predetermined broadcast limit has been reached.
 - D) A switch forwards a broadcast frame to another switch, which forwards the same frame to a third switch, which forwards it to a fourth switch, and so on until the predetermined broadcast limit has been reached.

- Q5) Why is it a problem for multiple copies of the same frame to arrive at a destination?
- A) because most protocols are not designed to cope with a multicast frame
 - B) because no protocols are designed to cope with multiple copies of a frame
 - C) because most protocols are designed to cope with multiple copies of a frame
 - D) because most protocols are not designed to cope with multiple copies of a frame
- Q6) How would a loop avoidance mechanism prevent multiple frame transmissions?
- A) by preventing one interface on one switch from transmitting frames during normal operation
 - B) by preventing one interface on each switch from transmitting frames during normal operation
 - C) by preventing all of the interfaces on one switch from transmitting or receiving frames during normal operation
 - D) by preventing all of the interfaces on all switches but one from transmitting or receiving frames during normal operation
- Q7) How could the MAC database on a switch become unstable after receiving the same frame on different ports?
- A) The switch creates an entry in the MAC database for each instance of the frame that it receives. The database can soon become very large, wasting the available resources of the switch.
 - B) The switch creates only a single entry in the MAC database for a frame from a specific address. As a result, the entry is based on the first frame received, and the port assignment might be incorrect.
 - C) The entry in the MAC database created when the first instance of the frame arrives will be replaced by a new entry when each subsequent frame arrives. The database entry could be rewritten repeatedly.
 - D) The switch creates an entry in the MAC database for each instance of the frame that it receives on a different port. With multiple entries in the database for a single address, forwarding and filtering decisions cannot be made properly.

Quiz Answer Key

- Q1) B, E
Relates to: Redundant Switched and Bridged Topologies
- Q2) D
Relates to: Redundant Switched and Bridged Topologies
- Q3) C
Relates to: Broadcast Storms
- Q4) A
Relates to: Broadcast Storms
- Q5) D
Relates to: Multiple Frame Transmissions
- Q6) A
Relates to: Multiple Frame Transmissions
- Q7) C
Relates to: MAC Database Instability

Spanning Tree Protocol Overview

Overview

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in switched or bridged networks. The STP operation is transparent to end stations. The STP runs on Layer 2 switches, bridges, and routers that are configured to operate as bridges. This lesson describes the functionality of the STP.

Relevance

Knowing the problems that are caused by redundant topologies in switched or bridged networks, you should know how STP can address such problems.

Objectives

Upon completing this lesson, you will be able to:

- Describe the purpose and operation of the STP
- Explain how to implement STP to solve the problems associated with redundant switched or bridged topologies

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

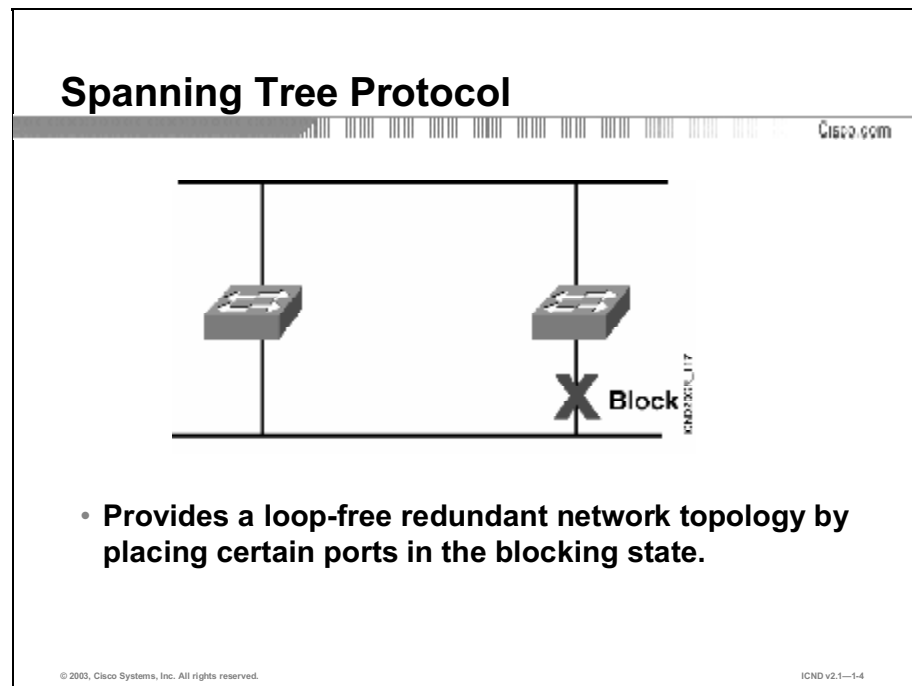
Outline

The lesson includes these topics:

- Overview
- Spanning Tree Protocol
- Spanning-Tree Operation
- Selecting the Root Bridge
- Stages of Spanning-Tree Port States
- Spanning-Tree Recalculation
- Rapid Spanning-Tree Protocol
- Summary
- Quiz

Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a Layer 2 link management protocol that is used to maintain a loop-free network. This topic describes the purpose and history of the STP.



STP was originally developed by the Digital Equipment Corporation (DEC). The DEC spanning-tree algorithm was subsequently revised by the IEEE 802 committee and published in the IEEE 802.1d specification. The DEC and the IEEE 802.1d algorithm are *not* the same and are *not* compatible. The Cisco switches, such as the Catalyst 1900 series and the Catalyst 2950 series, use the IEEE 802.1d STP.

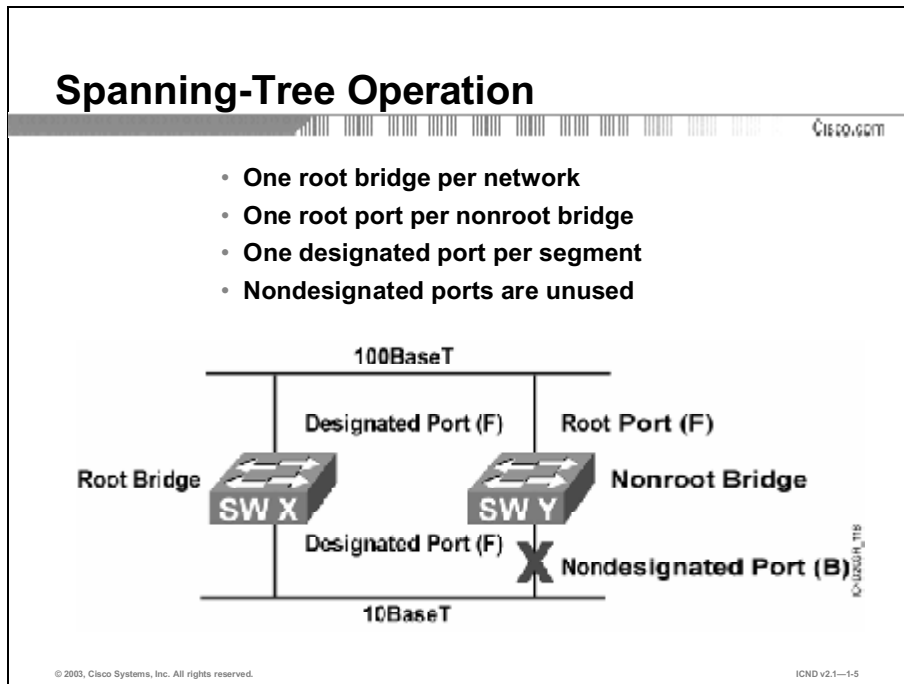
The purpose of STP is to maintain a loop-free network topology. A loop-free topology is accomplished when the switch or bridge recognizes a loop in the topology and logically blocks one or more redundant ports automatically.

The Spanning Tree Protocol continually probes the network so that the failure or addition of a link, switch, or bridge, is detected. When the network topology changes, the switches and bridges that are running STP automatically reconfigure their ports to avoid the loss of connectivity or the creation of loops.

STP is enabled by default in Catalyst switches.

Spanning-Tree Operation

The STP uses two key concepts when creating a loop-free logical topology. The two key concepts are bridge ID (BID) and path cost. This topic describes the STP operations.



The STP initially converges on a logically loop-free network topology by completing the following three steps:

1. **Elects one root bridge:** The STP has a process to elect a root bridge. Only one bridge can act as the root bridge in a given network. On the root bridge, all ports are designated ports. Designated ports are normally in the forwarding state. When in the forwarding state, a port can send and receive traffic. In the example, switch X is elected as the root bridge.
2. **Selects the root port on the nonroot bridges:** STP establishes one root port on the nonroot bridge. The root port is the lowest-cost path from the nonroot bridge to the root bridge. Root ports are normally in the forwarding state. Spanning-tree path cost is an accumulated cost calculated on the bandwidth. In the example, from switch Y, the lowest-cost path to the root bridge is through the 100BaseT Fast Ethernet link.
3. **Selects the designated port on each segment:** On each segment, STP establishes one designated port. The designated port is selected on the bridge that has the lowest path cost to the root bridge. Designated ports are normally in the forwarding state, forwarding traffic for the segment. In the example, the designated port for both segments is on the root bridge because the root bridge is directly connected to both segments. The 10BaseT Ethernet port on switch Y is a nondesignated port because there is only one designated port per segment. Nondesignated ports are normally in the blocking state to logically break the loop topology. When a port is in the blocking state, the port is not forwarding traffic but it can still receive traffic.

Selecting the Root Bridge

With STP, the root bridge is the bridge with the lowest BID. The BID includes the priority and MAC address of the bridge. This topic describes how the STP selects the root bridge.

Spanning Tree Protocol Root Bridge Selection

Cisco.com

Switch X
Default Priority 32768
(0x8000)
MAC 0c0011111111

SW X

BPDUs

SW Y

Switch Y
Default Priority 32768
(0x8000)
MAC 0c0022222222

- Bpdu = Bridge Protocol Data Unit
(default = sent every two seconds)
- Root bridge = Bridge with the lowest bridge ID
- Bridge ID =

Bridge Priority	MAC Address
- In this example, which switch has the lowest bridge ID?

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-6

Switches and bridges running the spanning-tree algorithm exchange configuration messages with other switches and bridges at regular intervals (every two seconds by default) using a multicast frame called the bridge protocol data unit (BPDU). One of the pieces of information included in the BPDU is the BID.

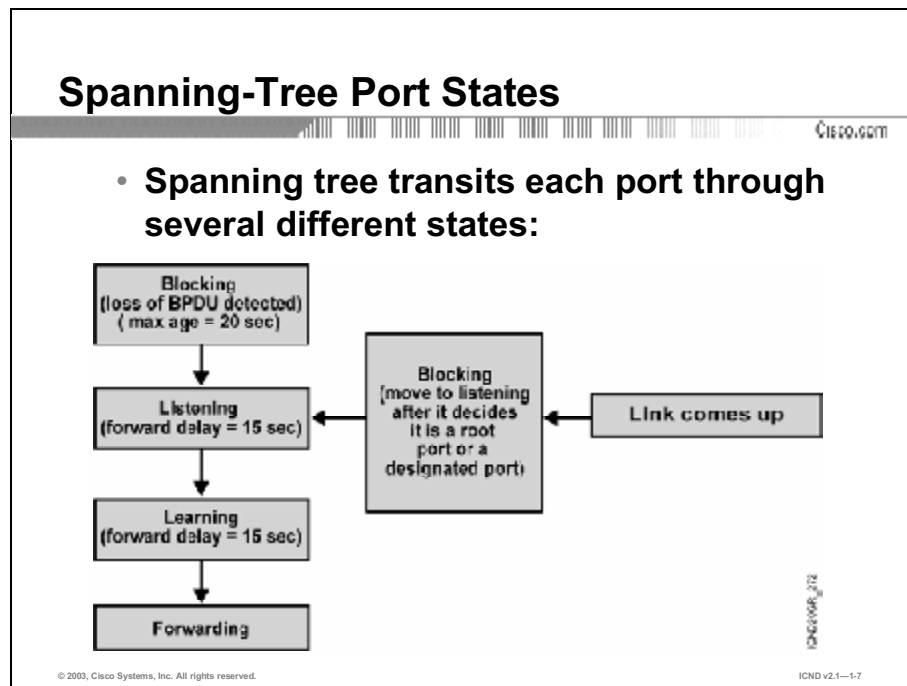
Spanning tree calls for each bridge to be assigned a unique BID. Typically, the BID is made up of a priority value (two bytes) and the bridge MAC address (six bytes). The default priority, in accordance with IEEE 802.1d, is 32,768 (1000 0000 0000 0000 in binary, or 0x8000 in hex), which is the midrange value. The root bridge is the bridge with the lowest BID.

Note A Cisco Catalyst switch uses one of its MAC addresses from a pool of MAC addresses that are assigned to either the backplane or to the supervisory module, depending on the switch model.

In the example, because both switches are using the same default priority, the one with the lowest MAC address will be the root bridge. In this example, switch X is the root bridge with a BID of 0x8000 (0c00.1111.1111).

Stages of Spanning-Tree Port States

With the STP, ports transition through four states: blocking, listening, learning, and forwarding. This topic describes the spanning-tree port states.



When STP is enabled, every bridge in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, the ports then stabilize to the forwarding or blocking state. Forwarding ports provide the lowest-cost path to the root bridge. Two transitional states occur when a bridge recognizes a change in the network topology. During a topology change, a port temporarily implements the listening and learning states.

Initially, all bridge ports start in the blocking state where they listen for BPDUs. When the bridge first boots up, it thinks it is the root bridge and will transition to the listening state. Or an absence of BPDUs for a certain period of time (the max_age) can cause a transition from the blocking state to the listening state. When a port is in the transitional listening state, it is able to send and receive BPDUs to determine the active topology. At this point, no user data is being passed. It is during the listening state that the bridge performs these three steps: electing the root bridge, electing the root ports on the nonroot bridges, and electing the designated ports on each segment.

Ports that remain as designated or root ports after 15 seconds (the forward delay) will transition to the learning state. Ports that are not the designated or root ports will transition back to the blocking state. When a port is in learning state, it is able to populate its MAC address table with MAC addresses heard on its ports, but it does not forward user frames. The learning state also lasts 15 seconds (also the forward delay) by default. At this point, the bridge is still not passing any user data.

The learning state reduces the amount of flooding required when data forwarding begins. If a port is still a designated or root port at the end of the learning state, the port will transition to

the forwarding state. Ports that are not the designated or root ports will transition back to the blocking state. In the forwarding state, a port is capable of sending and receiving user data.

The normal time it takes for a port to transition from the blocking state to the forwarding state is 30 to 50 seconds. Spanning-tree timers can be tuned to adjust the timing. Normally, these timers should be set to the default value. The default values are put in place to give the network enough time to gather all the correct information about the network topology.

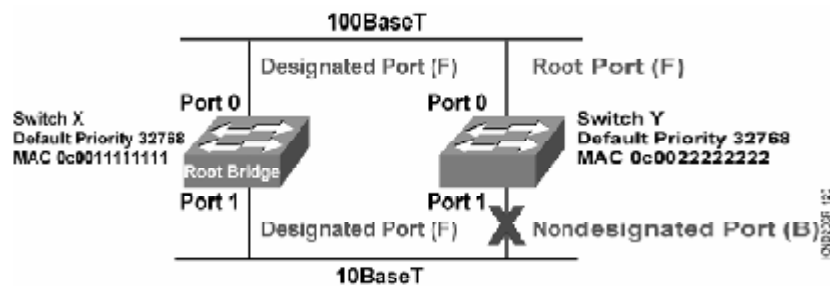
The time it takes for a port to transition from the listening state to the learning state, or from the learning state to the forwarding state, is called the forward delay. The forward delay has a default value of 15 seconds.

The max_age, which has a default value of 20 seconds, is the time a bridge stores a BPDU before discarding it. If a port is in blocking state and it does not receive a new BPDU within the max_age, it will transition from the blocking state to the listening state.

Note	If a switch port is connected only to end-user stations (<i>not</i> connected to another switch or bridge), you should enable a Catalyst switch feature called <i>PortFast</i> on those end-user ports. With PortFast, when the port first comes up, it will automatically transition from the blocking state to the forwarding state. This is acceptable because no loops can be formed through those ports because there are no other switches or bridges connected to it.

Spanning-Tree Port States (Cont.)

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-8

With the example topology, under STP, the following actions occur:

- The ports on switch X, the root bridge, are the designated ports (forwarding).
- The Fast Ethernet port on switch Y is the root port (forwarding). It has a lower path cost to the root bridge than the Ethernet port.
- The Ethernet port on switch Y is the nondesignated port (blocking). There is only one designated port per segment.

Spanning-Tree Path Cost

Cisco.com

Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

© 2003, Cisco Systems, Inc. All rights reserved.

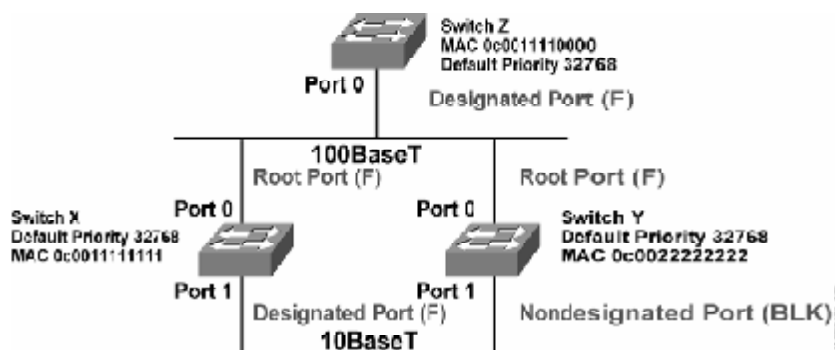
ICND v2.1—1-9

Spanning-tree path cost is an accumulated total path cost based on the bandwidth of all the links in the path. In the figure, some of the path costs specified in the IEEE 802.1d specification are shown. The IEEE 802.1d specification was revised; in the older specification, the cost was calculated based on 1000-Mbps bandwidth. The new specification adjusted the calculation using a nonlinear scale to accommodate higher-speed interfaces.

Note The current version of the Catalyst 1900 series software uses the older calculation for spanning-tree costs. Other Catalyst switches, including the Catalyst 2900 series XL, incorporate the revised cost calculations. A key point to remember about STP cost is that lower costs are better.

Spanning-Tree Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

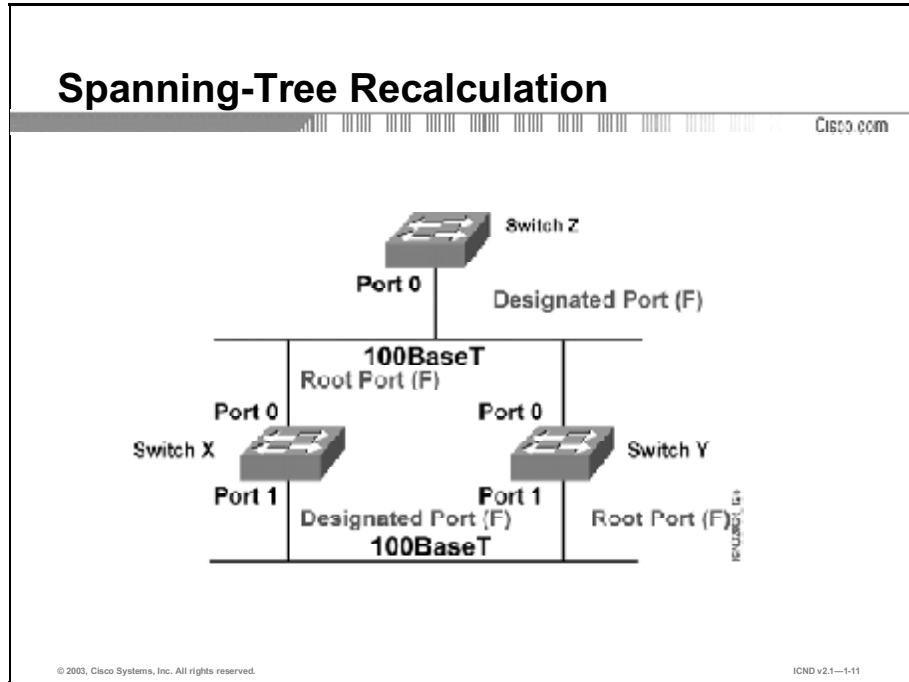
ICND v2.1—1-10

The following notes describe the example shown in the figure:

- The root bridge is switch Z, which has the lowest BID.
- The root port is port 0 on switches X and Y. It is the lowest-cost path to the root.
- The designated port is port 0 of switch Z. All ports on the root are designated ports. Port 1 of switch X is a designated port. Since both switch X and switch Y have the same path cost to the root bridge, the designated port is selected to be on switch X because it has a lower BID than switch Y.
- Blocking is the state of port 1 on switch Y, the nondesignated port on the segment.
- All designated and root ports are in the forwarding state.

Spanning-Tree Recalculation

If a change occurs to the network topology, the STP maintains connectivity by transitioning some blocked ports to the forwarding state. This topic describes how the STP adjusts the port states to accommodate topology changes.



When there is a topology change due to a bridge or link failure, the spanning tree readjusts the network topology to ensure connectivity by placing blocked ports in the forwarding states.

In the example, if switch X (the root bridge) fails and does not send a BPDU to switch X within the `max_age` (default is 20 seconds, which equals 10 missed BPDUs), switch Y will detect the missing BPDU from the root bridge. When the `max_age` timer on switch Y expires before a new BPDU has been received from switch X, a new spanning-tree recalculation is initiated. Switch Y will transition its blocking port (port 1) from the blocking state to the listening state to the learning state, then to the forwarding state.

After the network is converged, in about 50 seconds, switch Y will become the root bridge and will forward traffic between the two segments.

Spanning-Tree Convergence

Cisco.com

- **Convergence occurs when all the switch and bridge ports have transitioned to either the forwarding or the blocking state.**
- **When the network topology changes, switches and bridges must recompute the Spanning Tree Protocol, which disrupts user traffic.**

© 2003, Cisco Systems, Inc. All rights reserved.

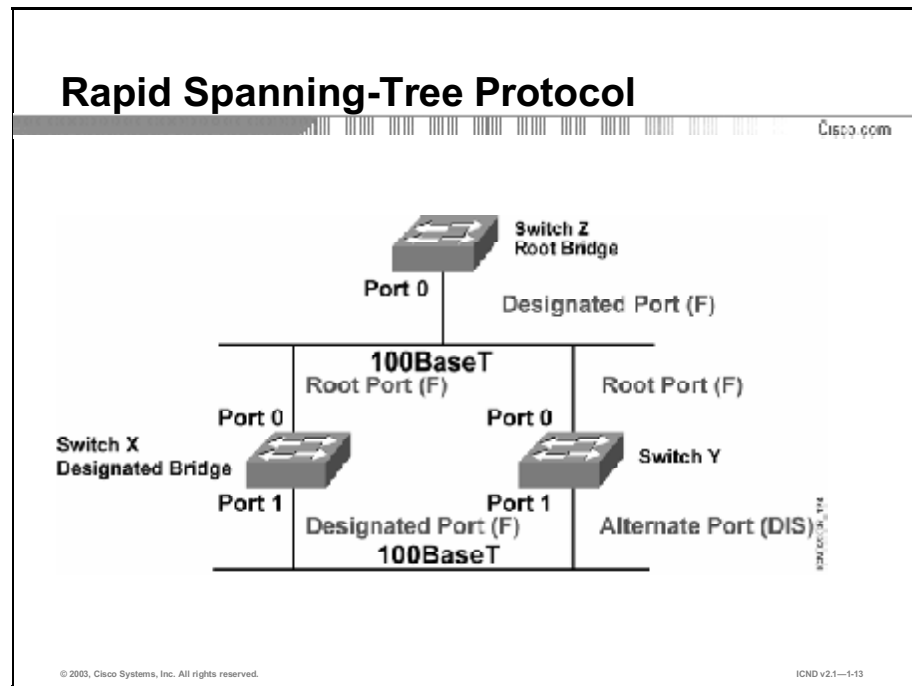
ICND v2.1—1-12

Convergence is a necessity for normal network operations. For a switched or bridged network, a key issue is the amount of time required for convergence when network topology changes. Convergence in STP means a state where all the switch and bridge ports have transitioned to either the forwarding or the blocking state.

Fast convergence is a desirable network feature because it reduces the period of time that bridges and switches have ports in transitional states and are not sending any user traffic. The normal convergence time can take from 30 to 50 seconds.

Rapid Spanning-Tree Protocol

Rapid Spanning-Tree Protocol (RSTP) is designed to significantly speed the recalculation of the spanning tree when the network topology changes. RSTP defines the additional port roles of alternate and backup, and defines port states as discarding, learning, or forwarding. This topic describes the differences between STP and RSTP.



RSTP (IEEE 802.1w) significantly reduces the time to reconverge the active topology of the network when changes to the physical topology or its configuration parameters occur.

RSTP selects one switch as the root of a spanning-tree-connected active topology and assigns port roles to individual ports on the switch, depending on whether the ports are part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding through an explicit handshake between them. RSTP allows switch port configuration so that the ports can transition to forwarding directly when the switch reinitializes.

RSTP, specified in IEEE 802.1w, supersedes STP specified in 802.1d, while remaining compatible with STP.

RSTP uses the following definitions for port roles:

- **Root:** A forwarding port elected for the spanning-tree topology.
- **Designated:** A forwarding port elected for every switched LAN segment.
- **Alternate:** An alternate path to the root bridge to that provided by the current root port.
- **Backup:** A backup for the path provided by a designated port toward the leaves of the spanning tree. Backup ports can exist only where two ports are connected together in a loopback by a point-to-point link or bridge with two or more connections to a shared LAN segment.
- **Disabled:** A port that has no role within the operation of spanning tree.

A root port or designated port role includes the port in the active topology. An alternate port or backup port role excludes the port from the active topology.

RSTP Port States

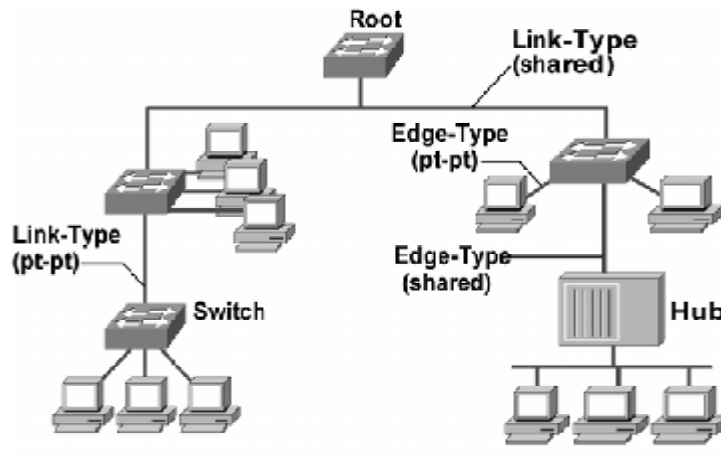
The port state controls the forwarding and learning processes and provides the values of discarding, learning, and forwarding. The table compares STP port states with RSTP port states.

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

In a stable topology, RSTP ensures that every root port and designated port transitions to forwarding while all alternate ports and backup ports are always in the discarding state.

Rapid Transition to Forwarding

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-14

The rapid transition is the most important feature introduced with IEEE 802.1w. Before the introduction of 802.1w, the spanning-tree algorithm waited passively for the network to converge before transitioning a port to the forwarding state. The new RSTP actively confirms that a port can safely transition to forwarding *without* relying on a timer configuration. To achieve fast convergence on a port, the protocol relies upon two new variables: edge port and link-type.

With edge ports, all ports directly connected to end stations cannot create bridging loops in the network and can, therefore, go directly to forwarding, skipping the listening and learning stages. An edge port does not generate topology changes when its link toggles.

RSTP is able to achieve rapid transition to forwarding only on edge ports and point-to-point (pt-pt) links. This is not a big constraint on the switched networks of today. The link-type is automatically derived from the duplex mode of a port. A port operating in full-duplex mode is point-to-point, while a port operating in half-duplex mode is considered *shared* by default. You can override the automatic link-type setting with an explicit configuration.

Note The figure does not represent a preferred design. It is simply an example of link types.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **STP is a bridge-to-bridge protocol used to maintain a loop-free network.**
- **STP establishes a root bridge, a root port, and designated ports.**
- **With STP, the root bridge has the lowest BID, which is made up of the bridge priority and MAC address.**
- **With STP, ports transition through four states: blocking, listening, learning, and forwarding.**
- **If a change occurs to the network topology, STP maintains connectivity by transitioning some blocked ports to the forwarding state.**
- **RSTP significantly speeds the recalculation of the spanning tree when the network topology changes.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-15

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the purpose of the STP?
- A) to maintain single loop paths
 - B) to maintain a loop-free network
 - C) to maintain a multiloop network
 - D) to maintain a reduced loop network
- Q2) When the network topology changes, ____.
- A) You must initiate a spanning-tree recalculation.
 - B) You must reconfigure the top node of the spanning tree.
 - C) You must reconfigure all devices participating in the spanning tree.
 - D) The STP reconfigures switch or bridge ports automatically.
- Q3) On the root bridge, all ports are ____.
- A) root ports
 - B) blocked ports
 - C) designated ports
 - D) nondesignated ports
- Q4) How does the STP select the root port on a nonroot bridge?
- A) Its root port is the highest-cost path from the nonroot bridge to the root bridge.
 - B) The root port is the lowest-cost path from the nonroot bridge to the root bridge.
 - C) The root port is the lowest-cost path from the nonroot bridge to the backup root bridge.
 - D) The root port is the highest-cost path from the nonroot bridge to the backup root bridge.
- Q5) Which bridge does the STP select as the root bridge?
- A) the one with the lowest priority
 - B) the one with the lowest BID
 - C) the one with the highest BID
 - D) the one with the highest MAC address

- Q6) What comprises the STP BID?
- A) bridge priority and bridge IP address
 - B) bridge priority and bridge MAC address
 - C) bridge MAC address and bridge IP address
 - D) bridge MAC address and Ethernet port number
- Q7) In what state can a port populate its MAC address table but not forward user frames?
- A) learning state
 - B) blocking state
 - C) listening state
 - D) forwarding state
- Q8) In the revised IEEE specification, what is the cost of a 100-Mbps link?
- A) 4
 - B) 10
 - C) 19
 - D) 100
- Q9) What is the definition of convergence for the STP?
- A) All the ports have transitioned to the blocking state.
 - B) All the ports have transitioned to the forwarding state.
 - C) All the ports have transitioned to either the forwarding or the listening state.
 - D) All the ports have transitioned to either the forwarding or the blocking state.
- Q10) What is the default max_age for the STP?
- A) 2 seconds
 - B) 15 seconds
 - C) 20 seconds
 - D) 30 seconds
- Q11) What is the RSTP equivalent state to the STP blocking state?
- A) blocking
 - B) dropping
 - C) discarding
 - D) forwarding

- Q12) Which port role specifies a forwarding port elected for every switched LAN segment when using the RSTP?
- A) root
 - B) backup
 - C) alternate
 - D) designated

Quiz Answer Key

- Q1) B
Relates to: Spanning Tree Protocol
- Q2) D
Relates to: Spanning Tree Protocol
- Q3) C
Relates to: Spanning-Tree Operation
- Q4) B
Relates to: Spanning-Tree Operation
- Q5) B
Relates to: Selecting the Root Bridge
- Q6) B
Relates to: Selecting the Root Bridge
- Q7) A
Relates to: Stages of Spanning-Tree Port States
- Q8) C
Relates to: Stages of Spanning-Tree Port States
- Q9) D
Relates to: Spanning-Tree Recalculation
- Q10) C
Relates to: Spanning-Tree Recalculation
- Q11) C
Relates to: Rapid Spanning-Tree Protocol
- Q12) D
Relates to: Rapid Spanning-Tree Protocol

Configuring a Catalyst Switch

Overview

A Cisco Catalyst switch comes with factory default settings. The default configuration will essentially set up the switch to function as a transparent bridge, with no management IP address, or default gateway or VLANs configured. You may want to change some of the default values to meet your specific goals. This lesson explains how to configure a Catalyst switch.

Relevance

Because every network is unique, you may need to modify some of the configuration parameters on your Catalyst switch.

Objectives

Upon completing this lesson, you will be able to:

- Verify the default configuration of the device, given a functioning access layer switch
- Configure the switch management IP address and the default gateway, given a functioning access layer switch and an IP addressing scheme
- Execute an add, move, or change on an access layer switch, given a new network requirement

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

Outline

The lesson includes these topics:

- Overview
- Verifying the Catalyst Switch Default Configuration
- Configuring the Catalyst Switch IP Address and Default Gateway
- Duplexing and Speed
- Configuring the Duplex Interface
- Managing the MAC Address Table
- Configuring Static MAC Addresses
- Configuring Port Security
- Executing Adds, Moves, and Changes
- Managing Device Configuration Files
- Summary
- Quiz

Verifying the Catalyst Switch Default Configuration

A Cisco Catalyst switch comes with factory default settings that can be displayed with the **show** command. This topic describes the default settings and how to display them.

Catalyst 1900 Series and 2950 Series Default Configuration



- **IP address: 0.0.0.0**
- **CDP: enabled**
- **100baseT port: autonegotiate duplex mode**
- **Spanning tree: enabled**
- **Console password: none**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-4

A Catalyst switch comes with factory default settings. For many parameters, the default configuration will suit your needs. However, you may want to change some of the default values to meet your specific network needs. The default values vary according to the features of the switch.

The figure lists some of the default settings on the Catalyst 1900 series and the Catalyst 2950 series switches. Not all of the defaults are shown in this example.

Port Names on Catalyst 1900 Series Switches

Cisco.com

```
wg_sw_1900#show run
```

```
Building configuration...
Current configuration:
!
interface Ethernet 0/1
!
interface Ethernet 0/2
```

```
wg_sw_1900#show spantree
```

```
Port Ethernet 0/1 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 32768, address 0090.8673.3340
Designated bridge has priority 32768, address 0090.8673.3340
Designated port is Ethernet 0/1, path cost 0
Timers: message age 20, forward delay 15, hold 1
```

```
wg_sw_1900#show vlan-membership
```

Port	VLAN	Membership Type	Port	VLAN	Membership Type
1	5	Static	13	1	Static
2	1	Static	14	1	Static
3	1	Static	15	1	Static

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-5

Ports on the Catalyst switches are referred to as either port or interface, depending on the context. For example, the following commands describe the port and interface conventions for the Catalyst 1900 series:

- The **show run** output refers to e0/1 as interface Ethernet 0/1.
- The **show spantree** output refers to e0/1 as port Ethernet 0/1.
- The **show vlan-membership** output refers to e0/1 as just port 1.

Port Names on Catalyst 2950 Series Switches

Cisco.com

```
wg_sw_2950#show run
```

```
Building configuration...
Current configuration:
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

```
wg_sw_2950#show spantree
```

```
Interface Fa0/1 (port 7) in Spanning tree 1 is FORWARDING
Port path cost 19, Port priority 128
Designated root has priority 32768, address 0008.a445.c980
Designated bridge has priority 32768, address 0008.a445.c980
Designated port is 7, path cost 0
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 8316, received 4
```

```
wg_sw_2950#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-6

The following commands describe the port and interface conventions for the Catalyst 2950 series switches:

- The **show run** output refers to fe0/1 as FastEthernet0/1.
- The **show spantree** output refers to fe0/1 as Interface Fa0.
- The **show vlan** output refers to fe0/1 as port Fa0/1.

Configuring the Catalyst Switch IP Address and Default Gateway

If the switch is to be a manageable entity on the network, it must have a basic IP configuration. To configure an IP address and subnet mask on the Catalyst 1900 series switch, use the **ip address** command. On the Catalyst 2950 series switch, you must configure an IP address and subnet mask for each interface. To configure a default gateway, use the **ip default-gateway** command. This topic describes how to set and reset the IP address, subnet mask, and default gateway for a Catalyst switch.

Configuring the Switch IP Address

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900(config)#ip address {ip_address} {mask}
```

- Configures an IP address and subnet mask on the switch

```
wg_sw_1900(config)#ip address 10.5.5.11 255.255.255.0
```

Catalyst 2950 Series

```
wg_sw_2950(config-if)#ip address {ip_address} {mask}
```

- Configures an IP address and subnet mask for the switch VLAN1 interface

```
wg_sw_2950(config)#interface vlan 1
wg_sw_2950(config-if)#ip address 10.5.5.11 255.255.255.0
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-7

To configure an IP address and subnet mask on the switch, use the **ip address** global configuration command. An IP address is required on the switch for management purposes.

For example, using the Virtual Switch Manager requires the switch to have an IP address configured and IP connectivity to communicate with a web browser, such as Netscape Communicator or Microsoft Internet Explorer. An IP address must also be assigned if you plan to connect to the switch via Telnet, or if you plan to use Simple Network Management Protocol (SNMP) to manage the switch.

Use the **no ip address** global configuration command to reset the IP address to the factory default of 0.0.0.0.

Configuring the Switch Default Gateway

Cisco.com

```
wg_sw_a(config)# ip default-gateway {ip address}
```

- Configures the switch default gateway for the Catalyst 1900 series and 2950 series switches

```
wg_sw_a(config)#ip default-gateway 10.5.5.3
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-8

Use the **ip default-gateway** global configuration command to configure the default gateway on both the Catalyst 1900 series and 2950 series switches. Use the **no ip default-gateway** command to delete a configured default gateway and set the gateway address to the default value of 0.0.0.0.

The switch is assigned an IP address for management purposes. If the switch needs to send traffic to a different IP network, the switch sends the traffic to the default gateway. The default gateway is the router IP address. A router is used to route traffic between different networks.

Showing the Switch IP Address

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#show ip
IP address: 10.5.5.11
Subnet mask: 255.255.255.0
Default gateway: 10.5.5.3
Management VLAN: 1
...
wg_sw_a#
```

Catalyst 2950 Series

```
wg_sw_2950#show interface vlan 1
Vlan1 is up, line protocol is up
Hardware is Cat5k Virtual Ethernet, address is 0010.f6a9.9800 (bia 0010.f6a9.9800)
Internet address is 172.16.80.79/24
Broadcast address is 255.255.255.255
. . .
wg_sw_2950#
```

© 2003, Cisco Systems, Inc. All rights reserved.

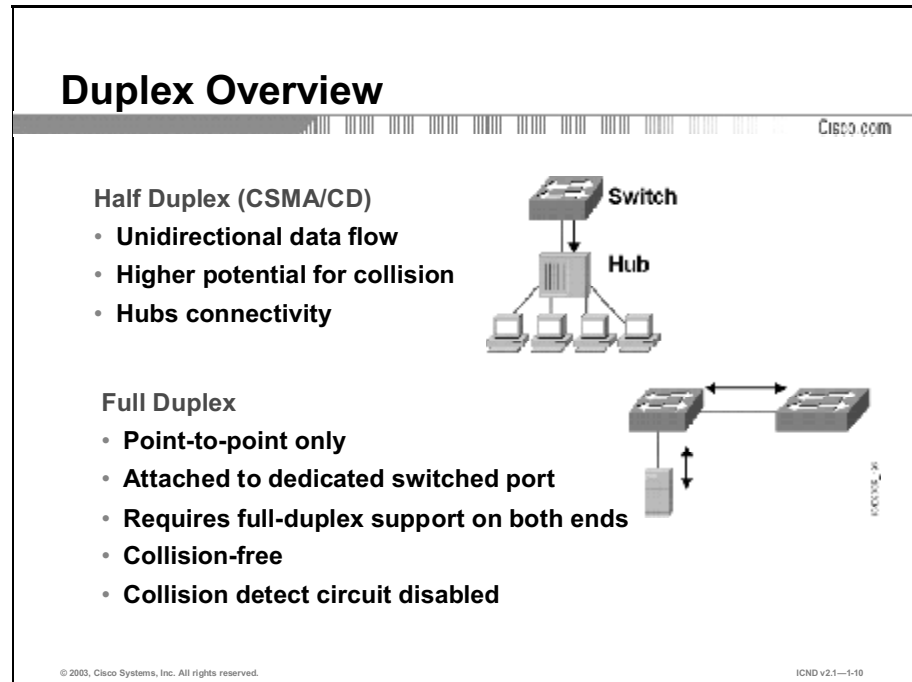
ICND v2.1—1-9

On the Catalyst 1900 series, use the **show ip** command from the privileged EXEC mode to verify the IP address, the subnet mask, and the default gateway settings.

On the Catalyst 2950 series, use the **show interface vlan** command to verify the IP address for each interface.

Duplexing and Speed

Half-duplex transmission uses collision detection. The faster full-duplex mode is used for directly connected devices where collision detection is unnecessary. This topic describes the two duplex modes.



Half-duplex transmission mode implements Ethernet carrier sense multiple access collision detect (CSMA/CD). The traditional shared LAN operates in half-duplex mode and is susceptible to transmission collisions across the wire.

Full-duplex Ethernet significantly improves network performance *without* the expense of installing new media. Full-duplex transmission between stations is achieved by using point-to-point Ethernet, Fast Ethernet, and Gigabit Ethernet connections. This arrangement is collision-free. Frames sent by the two connected end nodes cannot collide because they use two separate circuits in the Category 5 or Category 3 cable. Each full-duplex connection uses only one port.

Full-duplex port connections are point-to-point links between switches or end nodes, but not between shared hubs. Nodes that are directly attached to a dedicated switch port with Network Interface Cards (NIC) that support full duplex should be connected to switch ports configured to operate in full-duplex mode. Most Ethernet, Fast Ethernet, and Gigabit Ethernet NICs sold today offer full-duplex capability. In full-duplex mode, the collision detect circuit is disabled.

Nodes that are attached to hubs that share their connection to a switch port must operate in half-duplex mode because the end stations must be able to detect collisions.

Standard shared Ethernet configuration efficiency is typically rated at 50 to 60 percent of the 10-Mbps bandwidth. Full-duplex Ethernet offers 100 percent efficiency in both directions (10-Mbps transmit and 10-Mbps receive).

Configuring the Duplex Interface

Use the **duplex** command to configure switch duplex options. This topic describes how to set and view duplex options.

Setting Duplex Options



Catalyst 1900 Series

```
wg_sw_1900(config)#interface e0/1
wg_sw_1900(config-if)#duplex {auto | full |
full-flow-control | half}
```

Catalyst 2950 Series

```
wg_sw_2950(config)#interface fe0/1
wg_sw_2950(config-if)#duplex {auto | full | half}
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-11

Use the **duplex** interface configuration command to enable duplex mode for an interface. The **duplex** parameters on the Catalyst 1900 series are as follows:

- **auto** sets autonegotiation of duplex mode
- **full** sets full-duplex mode
- **full-flow-control** sets full-duplex mode with flow control
- **half** sets half-duplex mode

For 100-Mbps TX ports, the default setting is **duplex auto**. For all other ports that support half- and full-duplex, the default setting is **duplex half**.

The duplex parameters on the Catalyst 2950 series are as follows:

- **auto** sets autonegotiation of duplex mode
- **full** sets full-duplex mode
- **half** sets half-duplex mode

For Fast Ethernet and 10/100/1000 ports, the default is **auto**. For 100BaseFX ports, the default is **full**. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when set to 1000 Mbps, they operate only in full-duplex mode.

100BaseFX ports operate only at 100 Mbps in full-duplex mode.

Note To determine the default **duplex** mode settings for the Gigabit Interface Converter (GBIC)-module ports, refer to the documentation that came with your GBIC module.

Showing Duplex Options

Cisco.com

```
Switch#show interfaces fastethernet0/3

FastEthernet0/3 is up, line protocol is down
Hardware is Fast Ethernet, address is 0000.0000.0003 (bia 0000.0000.0003)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 10Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-12

Verify the duplex settings using the **show interfaces** command on both the Catalyst 1900 series and 2950 series. The **show interfaces** privileged EXEC command displays statistics and status for all or specified interfaces. One of the pieces of information shown is the duplex setting of an interface.

Autonegotiation can at times produce unpredictable results; for example, if an attached device does not support autonegotiation and is operating in full duplex, and if by default the Catalyst switch sets the corresponding switch port to half-duplex mode. This configuration, half duplex on one end and full duplex on the other, causes late collision errors at the half-duplex end. To avoid this situation, manually set the duplex parameters of the switch to match the attached device.

If the switch port is in full-duplex mode, and the attached device is in half-duplex mode, check for frame check sequence (FCS) errors on the switch full-duplex port.

You can use the **show interfaces** command to check for FCS for late collision errors.

Managing the MAC Address Table

MAC address tables include dynamic, permanent, and static addresses. Use the **mac-address-table** command to set permanent and static addresses. This topic describes how to manage the MAC address table.

Managing the MAC Address Table

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#show mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 6
```

Address	Dest	Interface	Type	Source Interface	List
00E0.1E5D.AE2F	Ethernet	0/2	Dynamic	All	
00D0.588F.B604	FastEthernet	0/26	Dynamic	All	
00E0.1E5D.AE2B	FastEthernet	0/26	Dynamic	All	
0090.273B.87A4	FastEthernet	0/26	Dynamic	All	
00D0.588F.B600	FastEthernet	0/26	Dynamic	All	
00D0.5892.38C4	FastEthernet	0/27	Dynamic	All	

Catalyst 2950 Series

```
wg_sw_2950#show mac-address-table
Dynamic Address Count:      1
Secure Address Count:      0
Static Address (User-defined) Count: 0
System Self Address Count: 25
Total MAC addresses:       26
Maximum MAC addresses:     8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0050.0f02.3372      Dynamic      1     FastEthernet0/2
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1-1-13

Switches use the MAC address tables to forward traffic between ports. These MAC tables include dynamic, permanent, and static addresses.

Dynamic addresses are source MAC addresses that are learned by the switch and then dropped when they are not refreshed and aged out. The switch provides dynamic addressing by learning the source MAC address of each frame it receives on each port and adding the source MAC address and its associated port number to the MAC address table. As stations are added or removed from the network, the switch updates the MAC address table, adding new entries and aging out those that are currently not in use.

An administrator can specifically assign permanent addresses to certain ports. Unlike dynamic addresses, permanent addresses are not aged out.

The maximum size of the MAC address table varies with different switches. For example, the Catalyst 1900 series switch can store up to a maximum of 1024 MAC addresses in its MAC address table, while the Catalyst 2950 series switch can store up to 8192 MAC addresses. When the MAC address table is full, traffic for all new unknown addresses are flooded.

Setting a Permanent MAC Address

Cisco.com

Catalyst 1900 Series and 2950 Series

```
wg_sw_1900(config)#mac-address-table permanent {mac-address  
type module/port}
```

```
wg_sw_1900(config)#mac-address-table permanent 2222.2222.2222 ethernet 0/3  
wg_sw_1900#show mac-address-table  
Number of permanent addresses : 1  
Number of restricted static addresses : 0  
Number of dynamic addresses : 4
```

Address	Dest	Interface	Type	Source Interface	List
00E0.1E5D.AE2F	Ethernet	0/2	Dynamic	All	
2222.2222.2222	Ethernet	0/3	Permanent	All	
00D0.588F.B604	FastEthernet	0/26	Dynamic	All	
00E0.1E5D.AE2B	FastEthernet	0/26	Dynamic	All	
00D0.5892.38C4	FastEthernet	0/27	Dynamic	All	

Catalyst 2950 Series Only

```
wg_sw_2950(config)#mac-address-table static  
mac_addr {vlan vlan_id} [interface int1 [int2 ... int15]]
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-14

Use the **mac-address-table permanent** global configuration command to associate a permanent MAC address with a particular switched port interface (specified by type and module/port) on the Catalyst 1900 series. Use the **no mac-address-table permanent** command to delete a permanent MAC address.

On the Catalyst 2950 series, use the **mac-address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the MAC address table. For example:

```
wg_sw_2950(config)#mac-address-table static 2222.2222.2222 int fa 0/1  
vlan 1
```

A permanent address in the MAC address table does not age out, and all interfaces can send traffic to it.

In the example, the command specifies that frames with the destination MAC address of 2222.2222.2222 should be forwarded on the Ethernet interface e0/3, and all interfaces can send traffic to 2222.2222.2222.

Configuring Static MAC Addresses

Use the **mac-address-table restricted static** command to associate a restricted static address with a particular port. This topic describes how to configure static MAC addresses.

Setting a Restricted Static MAC Address on the Catalyst 1900 Series

CISCO.COM

```
wg_sw 1900(config)#mac-address-table restricted static  
{mac-address type module/port src-if-list}
```

```
wg_sw 1900(config)#mac-address-table restricted static 1111.1111.1111 e0/4 e0/1  
wg_sw 1900#show mac-address-table  
Number of permanent addresses : 1  
Number of restricted static addresses : 1  
Number of dynamic addresses : 4
```

Address	Dest	Interface	Type	Source Interface List
1111.1111.1111	Ethernet	0/4	Static	Et0/1
00E0.1E5D.AE2F	Ethernet	0/2	Dynamic	All
2222.2222.2222	Ethernet	0/3	Permanent	All
00D0.588F.B604	FastEthernet	0/26	Dynamic	All
00E0.1E5D.AE2B	FastEthernet	0/26	Dynamic	All
00D0.5892.38C4	FastEthernet	0/27	Dynamic	All

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-15

Use the **mac-address-table restricted static** global configuration command on the Catalyst 1900 series to associate a restricted static address with a particular switched port interface. Use the **no mac-address-table restricted static** command to delete a restricted static address.

In the example, the switch allows traffic to the restricted static address 1111.1111.1111 on e0/4 only from interface e0/1.

Setting a Restricted Static MAC Address on the Catalyst 2950 Series

Cisco.com

```
wg_sw 2950(config)#mac-address-table secure  
hw-addr interface [vlan vlan-id]
```

```
wg_sw 2950#mac-address-table secure 0003.3333.3333 fa 0/1 vlan 1  
wg_sw 2950#show mac-address-table  
Dynamic Address Count:          1  
Secure Address Count:           1  
Static Address (User-defined) Count: 1  
System Self Address Count:      25  
Total MAC addresses:            28  
Maximum MAC addresses:          8192  
Non-static Address Table:  
Destination Address  Address Type  VLAN  Destination Port  
-----  
0050.0f02.3372      Dynamic      1    FastEthernet0/2  
0003.3333.3333      Secure       1    FastEthernet0/1  
  
Static Address Table:  
Destination Address  VLAN  Input Port  Output Ports  
-----  
2222.2222.2222      1    ALL         Fa0/1
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-16

Use the **mac-address-table secure** global configuration command on the Catalyst 2950 series to create a secure address. For example:

```
wg_sw 2950(config)#mac-address-table secure 0003.3333.3333 fa 0/1  
vlan 1
```

Configuring Port Security

Secured ports restrict the use of a port to a user-defined group of stations, set with the **port secure** command. This topic describes how to configure port security.

Configuring Port Security



Catalyst 1900 Series

```
wg_sw_1900(config-if)#port secure [max-mac-count count]
```

```
wg_sw_1900(config)#interface e0/4
wg_sw_1900(config-if)#port secure
wg_sw_1900(config-if)#port secure max-mac-count 1
```

Catalyst 2950 Series

```
wg_sw_2950(config-if)#port security max-mac-count count
```

```
wg_sw_2950(config)#interface fa0/1
wg_sw_2950(config-if)#port security
wg_sw_2950(config-if)#port security max-mac-count 10
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—1-17

On the Catalyst 1900 series, use the **port secure** interface configuration command to enable addressing security. Use the **no port secure** command to disable addressing security. Use the **no port secure max-mac-count** command to set the maximum number of addresses allowed on the interface to the default value (132).

On the Catalyst 2950 series, use the **port security** command to enable port security on a port and restrict the use of the port to a user-defined group of stations. Use the **port security max-mac-count** command to specify the maximum number of secure addresses supported by a secure port.

Secured ports restrict the use of a port to a user-defined group of stations. The number of devices on a secured port can range from 1 to 132. An administrator statically assigns the MAC addresses for the devices on a secure port, or the addresses are “sticky learned.” Sticky learning takes place when the address table for a secured port does not contain a full complement of static addresses. The port sticky learns the source address of incoming frames and automatically assigns them as permanent addresses.

Verifying Port Security on the Catalyst 1900 Series

Cisco.com

```
wg_sw_1900#show mac-address-table security
```

```
wg_sw_1900#show mac-address-table security  
Action upon address violation : Suspend
```

Interface	Addressing Security	Address Table Size
Ethernet 0/1	Disabled	N/A
Ethernet 0/2	Disabled	N/A
Ethernet 0/3	Disabled	N/A
Ethernet 0/4	Enabled	1
Ethernet 0/5	Disabled	N/A
Ethernet 0/6	Disabled	N/A
Ethernet 0/7	Disabled	N/A
Ethernet 0/8	Disabled	N/A
Ethernet 0/9	Disabled	N/A
Ethernet 0/10	Disabled	N/A
Ethernet 0/11	Disabled	N/A
Ethernet 0/12	Disabled	N/A

```
wg_sw_1900(config)#address-violation {suspend | disable | ignore}
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-18

On the Catalyst 1900 series, use the **show mac-address-table security** privileged EXEC command to display and verify the port security configurations.

On the Catalyst 1900 series, use the **address-violation** global configuration command to specify the action for a port address violation. Use the **no address-violation** command to set the switch to its default value (suspend). The **suspend** parameter suspends port on address violation. A suspended port is temporarily disabled until a certain number of frames with the proper address is received. The **disable** parameter disables a port on address violation. The **ignore** parameter ignores the address violation.

Verifying Port Security on the Catalyst 2950 Series

Cisco.com

```
wg_sw_2950#show mac-address-table secure
```

```
wg_sw_2950#show mac-address-table secure
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0003.3333.3333      Secure       1     FastEthernet0/1
```

```
wg_sw_2950(config-if)#port security action {shutdown | trap}
```

```
wg_sw_2950#show port-security
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-19

On the Catalyst 2950 series, use the **show port-security** privileged EXEC command to display the port security settings defined for an interface or for the switch. Use the **show mac-address-table secure** command to display the port security settings for an interface and the secure addresses in the MAC address table.

An address violation occurs when a secured port receives a source address that has been assigned to another secured port or when a port tries to learn an address that exceeds its address table size limit, set with the **port secure max-mac-count** command. When a security violation occurs, the action can be suspended, ignored, or disabled. When a port is suspended, it is re-enabled when a packet containing a valid address is received. When a port is disabled, it must be manually re-enabled. If the action is ignored, the switch ignores the security violation and keeps the port enabled.

On the Catalyst 2950 series, use the **port security action {shutdown | trap}** command to specify the action to take when an address violation occurs on a secure port. The default is **shutdown**.

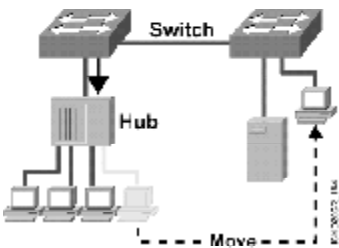
```
port security action trap
no port security action trap
port security action shutdown
no port security action shutdown
```


Executing Adds, Moves, and Changes

As your network topology changes by adding new devices or interfaces, or moving or changing existing ones, you may need to modify the switch configuration. This topic describes how to handle adds, moves, and changes for access layer switches.

Executing Adds, Moves, and Changes for MAC Addresses

Cisco.com



Adding a MAC Address

1. **Configure port security.**
2. **Configure the MAC address.**

Changing a MAC Address

1. **Remove MAC address restrictions.**

Moving a MAC Address

1. **Add the address to a new port.**
2. **Configure port security on the new switch.**
3. **Configure the MAC address to the port allocated for the new user**
4. **Remove the old port configuration.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—120

To add a new MAC address on an access switch that connects a workstation to the network, complete the following tasks:

1. Configure port security.
2. Configure the MAC address to the port allocated for the new interface so that the first MAC address seen on the port is the only address permitted.

To delete a MAC address on an access switch that connects a workstation to the network, complete the following tasks:

1. Remove the MAC address restrictions from the port.

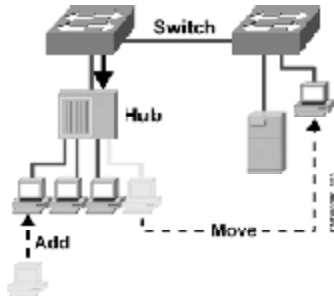
To move a MAC address from one access switch to another, you will delete the MAC address from one physical segment/logical network and assign it to a new physical segment. To move a MAC address, complete the following tasks:

1. Add the address to the new physical port.
2. On the new access switch, configure port security.
3. On the new access switch, configure the MAC address to the port allocated for the new user.
4. When all security is in place for the new location, shut down the old port and remove any MAC restrictions. Remove any old access lists from the original access switch.

If an Ethernet NIC fails, that MAC address is no longer valid because MAC addresses are unique. Installing a new Ethernet NIC will not permit access to the network for the affected workstation because the security policy is based on the old MAC address. In this case the only changes that need to be made are to the switch itself to remove the old MAC address from the security on the port and to add the new MAC address to the security on the port.

Adding a New Switch to the Network

Cisco.com



1. **Determine the IP address for management purposes.**
2. **Configure administrative access for the console, auxiliary, and vty interfaces.**
3. **Configure security for the device.**
4. **Configure the access switch ports as necessary.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-21

To add a new access switch to the network, complete the following tasks:

1. Configure the switch IP address and the default gateway to be used for management purposes.
2. Configure administrative access for the console, auxiliary, and vty, as appropriate.
3. Configure security for the device: There are two levels of security that need to be considered, the user EXEC level and the privileged EXEC level.
4. Configure the access switch ports as necessary to support single workstations, IP phones, and trunking to upstream/downstream switches.

Does the new switch have the potential to become the root of the spanning tree? To ensure that the new switch does *not* become the root, increase the priority value. Connect the switch into the existing infrastructure only after you have completed all of the switch configuration steps.

In moving equipment from one location to another, it may be easiest to treat it as both a removal and adding of equipment, depending on the number of configuration changes required. If there are few administrative and interface changes, you can overwrite those specific configuration parameters. If the equipment is being moved to a site with few or no similar configuration settings, you should erase the configuration and proceed as if you are adding a new network device.

Managing Device Configuration Files

The **copy** command can be used to copy a configuration from or to a file server, while the **delete nvram** command resets the switch configuration to the factory default settings. This topic describes how to manage Catalyst switch configuration files.

Managing the Configuration File

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#copy nvram tftp://host/dst_file
```

```
wg_sw_1900#copy tftp://host/src_file nvram
```

```
wg_sw_1950#copy nvram tftp://10.1.1.1/wgswd.cfg
Configuration upload is successfully completed

wg_sw_1950#copy tftp://10.1.1.1/wgswd.cfg nvram
TFTP successfully downloaded configuration file
```

Catalyst 2950 Series

```
wg_sw_2950#copy startup-config tftp://host/dst_file
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-22

On the Catalyst 1900 series, use the **copy nvram tftp** privileged EXEC command to upload the running configuration to a TFTP server. Use the **copy tftp nvram** privileged EXEC command to download a configuration file from the TFTP server.

On the Catalyst 2950 series, use the **copy startup-config tftp:** command to upload the running configuration to a TFTP server.

Note On the Cisco Catalyst switches, the running configuration is automatically saved to nonvolatile RAM (NVRAM) whenever a change is made to the running configuration.

Clearing NVRAM

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#delete nvram
```

- Resets the system configuration to factory defaults

Catalyst 2950 Series

```
wg_sw_2950#erase startup-config
```

- Resets the system configuration to factory defaults

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-23

On the Catalyst 1900 series, use the **delete nvram** privileged EXEC command to reset the switch configuration to the factory defaults.

On the Catalyst 2950 series, use the **erase startup-config** privileged EXEC command to reset the switch configuration to the factory defaults.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- A Catalyst switch comes with factory default settings that can be displayed with the show command.
- To configure an IP address and subnet mask on a switch, use the ip address command. To configure a default gateway, use the ip default-gateway command.
- Half-duplex transmission uses collision detection. The faster full-duplex mode is used for directly connected devices where collision detection is not needed.
- Use the duplex command to configure switch duplex options.
- MAC address tables include dynamic, permanent, and static addresses. Use the mac-address-table command to set permanent and static addresses.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-24

Summary (Cont.)

Cisco.com

- Use the mac-address-table restricted static command to associate a restricted static address with a particular port.
- Secured ports restrict the use of a port to a user-defined group of stations, set with the port secure command.
- As your network endpoint topology changes by adding new devices or interfaces, or moving or changing existing ones, you may need to modify the switch configuration.
- The copy command can be used to copy a configuration from or to a file server, while the delete nvram command resets the switch configuration to the factory default settings.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—1-25

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Next Steps

After completing this lesson, go to:

- Lab Exercise 1-1: Cisco Remote Lab Connection
- Lab Exercise 1-2: Configuring the Switch

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What is the default IP address for the Catalyst 1900 series and 2950 series switches?
- A) 0.0.0.0
 - B) 1.1.1.1
 - C) 2.2.2.2
 - D) 3.3.3.3
- Q2) What is the default console password for the Catalyst 1900 series and 2950 series switches?
- A) cisco
 - B) catalyst
 - C) the word "none"
 - D) there is no default password
- Q3) Which Cisco IOS command returns the Catalyst 1900 series and 2950 series switch default gateway address to the factory default?
- A) **no ip default-gateway**
 - B) **ip no default-gateway**
 - C) **ip no-default-gateway**
 - D) **ip default-gateway 0.0.0.1**
- Q4) Which Cisco IOS command displays the IP address, subnet mask, and default gateway settings for a Catalyst 1900 series switch?
- A) **show ip**
 - B) **show default**
 - C) **show subnet**
 - D) **show address**
- Q5) What form of Ethernet can you use on nodes attached to hubs that share their connection to a switch port?
- A) full-duplex
 - B) half-duplex
 - C) either half- or full-duplex
 - D) both half- and full-duplex

- Q6) What efficiency does the full-duplex Ethernet interface on a Catalyst switch offer?
- A) Full-duplex Ethernet offers 100 percent efficiency in both directions.
 - B) Full-duplex Ethernet offers about 50 to 60 percent efficiency in both directions.
 - C) Full-duplex Ethernet offers 100 percent efficiency in only one direction, from a server to the switch.
 - D) Full-duplex Ethernet offers about 50 to 60 percent efficiency in only one direction, from a server to the switch.
- Q7) What does the command **duplex auto** do?
- A) sets full-duplex mode
 - B) sets half-duplex mode
 - C) sets autonegotiation of duplex mode
 - D) sets full-duplex mode with flow control
- Q8) What type of errors can indicate a duplex mode mismatch?
- A) address violations
 - B) runt and giant errors
 - C) jabber and alignment errors
 - D) FCS and late collision errors
- Q9) What type of MAC address is learned automatically by the switch?
- A) static
 - B) learned
 - C) dynamic
 - D) permanent
- Q10) What happens if a frame arrives at a switch destined for a MAC address that is not already in the MAC table, and the table is full?
- A) the frame is dropped
 - B) the frame is returned
 - C) the frame is forwarded through all ports
 - D) the frame is forwarded through all ports except the receiving port
- Q11) Which statement best describes a restricted static address?
- A) A restricted static address will age out.
 - B) A restricted static address is learned automatically by the switch.
 - C) A restricted static address allows frames from any other port to be forwarded to the specified port.
 - D) A restricted static address allows frames from only one or more specific ports to be forwarded to another specified port.

- Q12) Which command specifies that traffic to the address 1111.2222.1111 on e0/3 will be allowed only from interface e0/1 or e0/2 ?
- A) **mac-address-table restricted static 1111.2222.1111 e0/3 e0/1 e0/2**
 - B) **mac-address-table restricted static 1111.2222.1111 e0/1 e0/2 e0/3**
 - C) **mac-address-table restricted static 1111.2222.1111 e0/1 e0/3 e0/2**
 - D) **mac-address-table restricted static 1111.2222.1111 e0/2 e0/1 e0/3**
- Q13) What constitutes a port security address violation?
- A) when a secured port sticky learns the destination MAC address of incoming frames
 - B) when a secured port receives a frame with a destination MAC address that has not been assigned in the MAC address table
 - C) when a secured port tries to learn an address that exceeds its address table size limit using the **port secure max-mac-count** command
 - D) when a secured port sticky learns the source MAC address of incoming frames and automatically assigns them as permanent addresses
- Q14) Which commands set the maximum number of MAC addresses allowed in the MAC address table for port e0/1 to 5 on a Catalyst 1900 series switch?
- A) **int e0/1**
port secure
 - B) **int e0/1**
port secure 5
 - C) **int e0/1**
port secure mac-address 5
 - D) **int e0/1**
port secure max-mac-count 5
- Q15) Why would a replacement NIC NOT be granted access to the network through the switch?
- A) because the security policy is based on the old IP address
 - B) because the security policy is based on the new IP address
 - C) because the security policy is based on the old MAC address
 - D) because the security policy is based on the new MAC address
- Q16) Which Cisco IOS command downloads a Catalyst 1900 series switch configuration file from a TFTP server into the NVRAM?
- A) **copy tftp flash**
 - B) **copy nvram tftp**
 - C) **copy tftp nvram**
 - D) **copy flash nvram**

- Q17) Which Cisco IOS command resets the Catalyst 1900 series switch configuration to the factory defaults?
- A) **reset**
 - B) **delete**
 - C) **reset nvram**
 - D) **delete nvram**

Quiz Answer Key

- Q1) A
Relates to: Verifying the Catalyst Switch Default Configuration
- Q2) D
Relates to: Verifying the Catalyst Switch Default Configuration
- Q3) A
Relates to: Configuring the Catalyst Switch IP Address and Default Gateway
- Q4) A
Relates to: Configuring the Catalyst Switch IP Address and Default Gateway
- Q5) B
Relates to: Duplexing and Speed
- Q6) A
Relates to: Duplexing and Speed
- Q7) C
Relates to: Configuring the Duplex Interface
- Q8) D
Relates to: Configuring the Duplex Interface
- Q9) C
Relates to: Managing the MAC Address Table
- Q10) D
Relates to: Managing the MAC Address Table
- Q11) D
Relates to: Configuring Static MAC Addresses
- Q12) A
Relates to: Configuring Static MAC Addresses
- Q13) C
Relates to: Configuring Port Security
- Q14) D
Relates to: Configuring Port Security
- Q15) C
Relates to: Executing Adds, Moves, and Changes
- Q16) C
Relates to: Managing Device Configuration Files
- Q17) D
Relates to: Managing Device Configuration Files

Lesson Assessments

Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

Outline

This section includes these assessments:

- Lesson Assessment 1-1: Basic Layer 2 Switching and Bridging Functions
- Lesson Assessment 1-2: Redundant Topology Overview
- Lesson Assessment 1-3: Spanning Tree Protocol Overview
- Lesson Assessment 1-4: Configuring a Catalyst Switch

Lesson Assessment 1-1: Basic Layer 2 Switching and Bridging Functions

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe Layer 2 switching and bridging operations and modes
- Describe how LAN switches use and populate the MAC address table

Quiz

Answer these questions:

- Q1) Which two functions can LAN switches and bridges provide? (Choose two.)
- A) packet routing
 - B) jitter avoidance
 - C) address learning
 - D) store and forward decision
 - E) loop avoidance using the Spanning Tree Protocol
- Q2) Ethernet switching or bridging _____ the available bandwidth of a network by creating _____ network segments.
- A) increases, shared
 - B) decreases, shared
 - C) increases, dedicated
 - D) decreases, dedicated
- Q3) Which frame transmission mode reads the destination address of a frame only before forwarding it?
- A) cut-through
 - B) fragment-free
 - C) store and forward
 - D) All transmission modes read the destination address only before forwarding it.
- Q4) The fragment-free transmission mode forwards a frame immediately after reading _____.
- A) the entire frame
 - B) the destination address
 - C) the first 32 bytes of the frame
 - D) the first 64 bytes of the frame

- Q5) What feature do switches and bridges implement so that they can receive and transmit frames independently on each port?
- A) loop avoidance
 - B) buffering memory
 - C) store and forward mode
 - D) Spanning Tree Protocol
- Q6) Collisions usually happen within the first _____ bytes of a frame.
- A) 16
 - B) 32
 - C) 64
 - D) 128
- Q7) If a new MAC table entry is not _____ within a time limit, the entry is discarded.
- A) written to NVRAM
 - B) echoed to the sending station for confirmation
 - C) refreshed by a new frame sent to the same address on the same port
 - D) refreshed by a new frame received from the same address on the same port
- Q8) What information in a frame does a switch or bridge use to make frame forwarding decisions?
- A) source port
 - B) source address
 - C) destination port
 - D) destination address
- Q9) When a frame arrives with a known destination address, where does the switch or bridge forward it?
- A) the source port
 - B) the broadcast port
 - C) the destination port
 - D) all ports except the source port
- Q10) Which three frame types are flooded to all ports except the source port on a switch? (Choose three.)
- A) unicast frames
 - B) multicast frames
 - C) broadcast frames
 - D) frames with a known destination address
 - E) frames with an unknown destination address

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 1-2: Redundant Topology Overview

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features of redundant switch and bridge topologies
- Explain the problems associated with broadcast storms, multiple frame transmissions, and MAC address table instability
- Describe loop avoidance and explain how it can solve redundant switch topology issues

Quiz

Answer these questions:

- Q1) Which two problems are associated with redundant switched or bridged network designs? (Choose two.)
- A) broadcast floods
 - B) broadcast storms
 - C) MAC address table overflow
 - D) MAC address table instability
- Q2) Endlessly flooding or looping frames are commonly called ____.
- A) a flood storm
 - B) loop overload
 - C) a broadcast storm
 - D) broadcast overload
- Q3) What problem can arise from a switch or bridge receiving copies of the same frame on different ports?
- A) MAC table division
 - B) MAC table overflow
 - C) MAC table instability
 - D) MAC table underflow
- Q4) Switches and bridges flood broadcast frames onto ____.
- A) no ports
 - B) all ports
 - C) all ports except one random port
 - D) all ports except the receiving port
- Q5) What is the result of multiple copies of the same frame arriving at a destination?
- A) The result cannot be predicted.
 - B) The frame is ignored completely.
 - C) Every copy but the last is ignored.
 - D) Every copy but the first is ignored.

- Q6) Instability in the MAC address table results from what situation?
- A) a source address being learned from more than one port
 - B) a destination address being learned from more than one port
 - C) a source address being learned from the same port more than once
 - D) a destination address being learned from the same port more than once

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 1-3: Spanning Tree Protocol Overview

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the purpose and operation of the Spanning Tree Protocol (STP)
- Explain how to implement STP to solve the problems associated with redundant switched or bridged topologies

Quiz

Answer these questions:

- Q1) When does the STP automatically reconfigure switch or bridge ports?
- A) when the network topology changes
 - B) when the forward delay timer expires
 - C) when an administrator specifies a recalculation
 - D) when a new BPDU is not received within the forward delay
- Q2) How does the STP provide a loop-free network?
- A) by placing all ports in the blocking state
 - B) by placing all bridges in the blocking state
 - C) by placing some ports in the blocking state
 - D) by placing some bridges in the blocking state
- Q3) Which port is the lowest-cost path from the nonroot bridge to the root bridge?
- A) root
 - B) blocking
 - C) designated
 - D) nondesignated
- Q4) With STP, how is the designated port selected on a segment?
- A) the port that has the lowest path cost to the root bridge
 - B) the port that has the highest path cost to the root bridge
 - C) the port that has the lowest path cost to the closest nonroot bridge
 - D) the port that has the highest path cost to the closest nonroot bridge
- Q5) What components (in the correct order) make up the STP bridge ID (BID)?
- A) six-byte priority plus two-byte MAC address
 - B) two-byte MAC address plus six-byte priority
 - C) six-byte MAC address plus two-byte priority
 - D) two-byte priority plus six-byte MAC address

- Q6) In the listening state, a port _____.
A) is able to check for BPDUs and populate the MAC table
B) is able to check for BPDUs, but not yet populate its MAC table
C) is able to populate its MAC table, but not yet forward user frames
D) is able to forward user frames, but not yet populate its MAC table
- Q7) In which state is a nondesignated port, typically?
A) blocking
B) learning
C) listening
D) forwarding
- Q8) In which state is a root port, typically?
A) blocking
B) learning
C) listening
D) forwarding
- Q9) In the revised IEEE STP specification, what is the cost of a 1-Gbps link?
A) 2
B) 4
C) 10
D) 19
- Q10) On which STP bridge are all ports designated ports?
A) root bridge
B) nonroot bridge
C) the bridge with the lowest priority
D) the bridge with the highest bridge ID
- Q11) The STP can detect a change in topology _____.
A) when BPDU is not received within two seconds
B) when a device does not respond to a handshake message
C) when the max_age timer has expired without receiving a BPDU
D) when a device does not respond quickly enough to a handshake request
- Q12) Which switched network issue does RSTP address?
A) network security
B) size of the network
C) redundant topology
D) speed of convergence
- Q13) What is the RSTP equivalent to the STP listening state?
A) blocking
B) listening
C) discarding
D) forwarding

Q14) With RSTP, which two port roles are included in the active topology?

- A) root and alternate
- B) root and designated
- C) alternate and backup
- D) designated and backup

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 1-4: Configuring a Catalyst Switch

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Verify the default configuration of the device, given a functioning access layer switch
- Configure the switch management IP address and the default gateway, given a functioning access layer switch and an IP addressing scheme
- Execute an add, move, or change on an access layer switch, given a new network requirement

Quiz

Answer these questions:

- Q1) Which Cisco IOS command displays interface e0/1 as port 1?
- A) **show run**
 - B) **show spantree**
 - C) **show running-config**
 - D) **show vlan-membership**
- Q2) Which Cisco IOS command sets a Catalyst switch IP address to 10.1.1.3 255.255.255.0?
- A) **ip address 10.1.1.3/24**
 - B) **ip address 10.1.1.3 255.255.255.0**
 - C) **ip address 10.1.1.3 mask 255.255.255.0**
 - D) **ip address 10.1.1.3 ip mask 255.255.255.0**
- Q3) Which Cisco IOS command specifies the default gateway for the switch?
- A) **gateway**
 - B) **ip gateway**
 - C) **default-gateway**
 - D) **ip default-gateway**
- Q4) A full-duplex connection ____.
- A) requires that a second wire be installed
 - B) requires the use of two ports on each device
 - C) offers 100 percent efficiency in both directions
 - D) can be used on devices connected to either a switch port or a hub port, as long as no other devices are on the same port

- Q5) Which two statements describe half-duplex operation? (Choose two.)
- A) collision-free
 - B) unidirectional
 - C) point-to-point only
 - D) collision detection disabled
 - E) higher potential for collision
- Q6) Which command displays FCS errors?
- A) **show fcs**
 - B) **show duplex**
 - C) **show interface**
 - D) **show interface errors**
- Q7) What type of errors can indicate a duplex mode mismatch on a Catalyst switch?
- A) jabber errors
 - B) alignment errors
 - C) address violations
 - D) late collision errors
- Q8) What does the **duplex full** command do?
- A) sets full-duplex mode for the switch
 - B) sets full-duplex mode for an interface
 - C) sets full-duplex mode with flow control for the switch
 - D) sets full-duplex mode with flow control for an interface
- Q9) If a Catalyst switch port is in autonegotiate mode and an attached device that does NOT support autonegotiation is operating in full-duplex mode, what will the switch do?
- A) disable the port
 - B) suspend the port
 - C) set the port to full-duplex
 - D) set the port to half-duplex
- Q10) How many addresses can you store in the Catalyst 1900 series MAC address table?
- A) 256
 - B) 512
 - C) 1024
 - D) 2048
- Q11) How many addresses can you store in the Catalyst 2950 series MAC address table?
- A) 512
 - B) 1024
 - C) 2048
 - D) 8192

- Q12) What does the **mac-address-table restricted static 1111.2222.1111 e0/3 e0/1** command do?
- A) associates the address 1111.2222.1111 with both ports e0/3 and e0/1
 - B) specifies that traffic to the address 1111.2222.1111 will be allowed only from interface e0/3 or e0/1
 - C) specifies that traffic to the address 1111.2222.1111 on e0/3 will be allowed only from interface e0/1
 - D) specifies that traffic to the address 1111.2222.1111 on e0/1 will be allowed only from interface e0/3
- Q13) Which two types of MAC addresses can an administrator assign manually on the Catalyst 1900 switch ports? (Choose two.)
- A) learned
 - B) dynamic
 - C) transitory
 - D) permanent
 - E) restricted static
- Q14) What constitutes a port security address violation?
- A) a secured port receives an unknown destination address
 - B) a secured port receives a source address that has already been assigned to that port
 - C) a secured port receives a source address that has been assigned to another secured port
 - D) a secured port receives an unknown source address and the max-mac-count for that port has not been reached
- Q15) Which command restricts port usage to no more than ten devices?
- A) **port secure 10**
 - B) **port max-mac-count 10**
 - C) **port secure max-mac-count 10**
 - D) **port secure 10 max-mac-count**
- Q16) What is the default maximum number of addresses allowed on a secure port?
- A) 48
 - B) 128
 - C) 132
 - D) 256
- Q17) Which Catalyst 1900 series command uploads the current configuration to a TFTP server?
- A) **copy tftp flash**
 - B) **copy nvram tftp**
 - C) **copy tftp nvram**
 - D) **copy flash nvram**

- Q18) Which Catalyst 2950 series command uploads the current configuration to a TFTP server?
- A) **copy tftp flash**
 - B) **copy nvram tftp**
 - C) **copy tftp nvram**
 - D) **copy startup-config tftp**
- Q19) What does the **delete nvram** command do on a Catalyst 1900 series switch?
- A) deletes the MAC address table on the switch
 - B) resets the switch configuration to the factory defaults
 - C) resets the switch configuration to the last-saved version
 - D) deletes all configuration information on the switch, including all the defaults
- Q20) What does the **erase startup-config** command do on a Catalyst 2950 series switch?
- A) deletes the MAC address table on the switch
 - B) resets the switch configuration to the factory defaults
 - C) resets the switch configuration to the last-saved version
 - D) deletes all configuration information on the switch, including all the defaults

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment Answer Key

Lesson Assessment 1-1: Basic Layer 2 Switching and Bridging Functions

- Q1) C, E
- Q2) C
- Q3) A
- Q4) D
- Q5) B
- Q6) C
- Q7) D
- Q8) D
- Q9) C
- Q10) B, C, E

Lesson Assessment 1-2: Redundant Topology Overview

- Q1) B, D
- Q2) C
- Q3) C
- Q4) D
- Q5) A
- Q6) A

Lesson Assessment 1-3: Spanning Tree Protocol Overview

- Q1) A
- Q2) C
- Q3) A
- Q4) A
- Q5) D
- Q6) B
- Q7) A
- Q8) D
- Q9) B
- Q10) A
- Q11) C
- Q12) D
- Q13) C
- Q14) B

Lesson Assessment 1-4: Configuring a Catalyst Switch

- Q1) D
- Q2) B
- Q3) D
- Q4) C
- Q5) B, E
- Q6) C
- Q7) D
- Q8) B
- Q9) D
- Q10) C
- Q11) D
- Q12) C
- Q13) D, E
- Q14) C
- Q15) C
- Q16) D
- Q17) B
- Q18) D
- Q19) B
- Q20) B

Extending Switched Networks with VLANs

Overview

A virtual LAN (VLAN) is a group of end stations with a common set of requirements, independent of their physical location. A VLAN has the same attributes as a physical LAN, but allows you to group end stations even if they are not physically located on the same LAN segment. VLANs allow you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN floods only ports belonging to that VLAN. This module describes the features and operation of VLANs, and shows you how to configure and troubleshoot them.

Upon completing this module, you will be able to:

- Use Cisco IOS commands to configure VLANs, VLAN Trunking Protocol, IEEE 802.1Q trunking, and Inter-Switch Link trunking, given a functioning access layer switch
- Execute an add, move, or change on an access layer switch, given a new network requirement
- Use **show** commands to identify anomalies in VLAN, VLAN Trunking Protocol, Inter-Switch Link trunking, and spanning-tree operations, given an operational access layer switch
- Use **debug** commands to identify events and anomalies in VLAN, VLAN Trunking Protocol, Inter-Switch Link trunking, and spanning-tree operations, given an operational access layer switch

Outline

The module contains these lessons:

- VLAN Operation Overview
- Configuring VLANs
- Lesson Assessments

VLAN Operation Overview

Overview

Cisco Systems provides virtual LAN (VLAN)-capable solutions across its suite of internetworking switches and routers. Not only do VLANs solve many of the immediate problems associated with administrative changes, they also provide scalability, interoperability, and increased dedicated throughput. This lesson describes VLAN operations and its associated protocols.

Relevance

You must understand how VLANs operate and the important VLAN protocols in order to configure, verify, and troubleshoot VLANs on Cisco access switches.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of a VLAN, VLAN Trunking Protocol, IEEE 802.1Q trunking, and Inter-Switch Link trunking

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

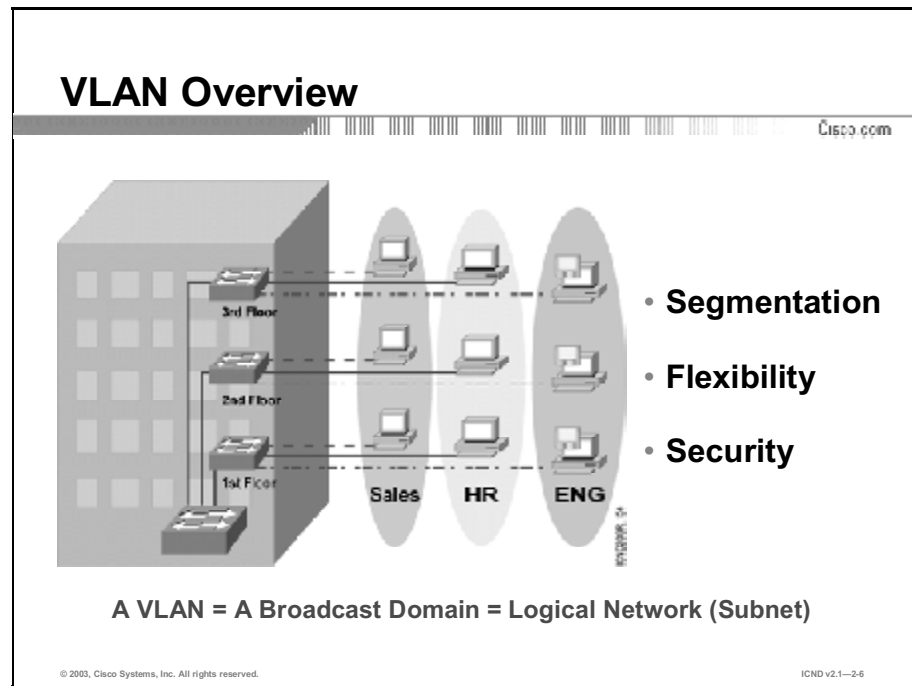
Outline

The lesson includes these topics:

- Overview
- Defining a VLAN
- VLAN Operation
- VLAN Membership Modes
- 802.1Q Trunking
- ISL Protocol and Encapsulation
- VTP Protocol Features
- VTP Modes, Operation, and Pruning
- Summary
- Quiz

Defining a VLAN

A VLAN permits a group of users to share a common broadcast domain regardless of their physical location in the internetwork. Creating VLANs improves performance and security in the switched network by controlling broadcast propagation. This topic introduces the basic capabilities that VLANs offer.



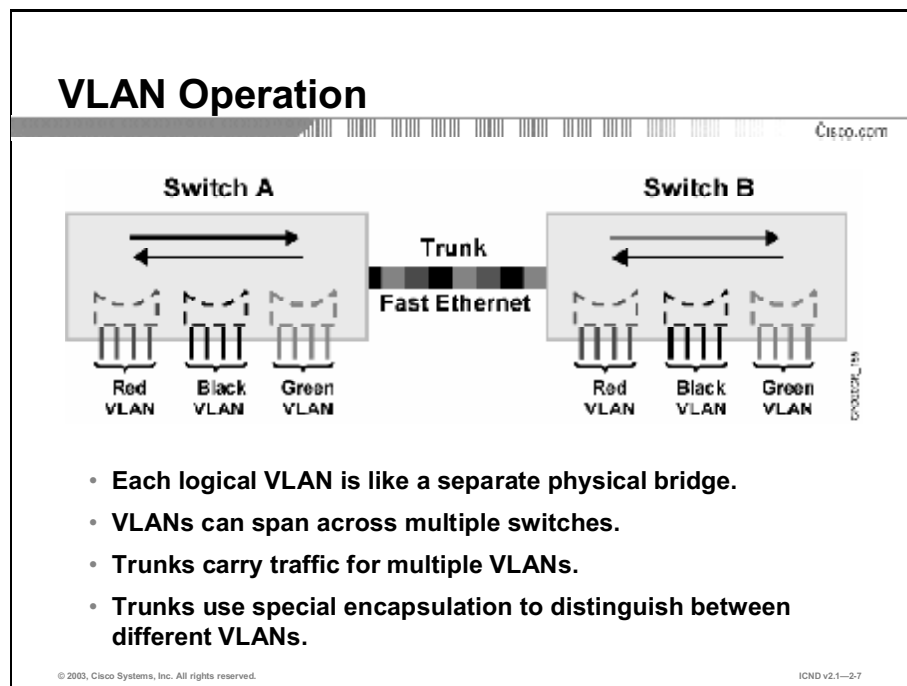
A VLAN is a logical broadcast domain that can span multiple physical LAN segments. You can design a VLAN to establish stations that are segmented logically by functions, project teams, or applications without regard to the physical location of users. You can assign each switch port to only one VLAN. Ports in a VLAN share broadcasts; ports in different VLANs do *not* share broadcasts. This improves the overall performance of the network.

Within the switched internetwork, VLANs provide segmentation and organizational flexibility. Using VLAN technology, you can group switch ports and their connected users into logically defined communities, such as coworkers in the same department, a cross-functional product team, or diverse user groups sharing the same network application.

A VLAN can exist on a single switch or span multiple switches. It can include stations in a single building or multiple-building infrastructures, or it can connect across WANs.

VLAN Operation

A Cisco Catalyst switch operates in a network like a traditional bridge. Each VLAN configured on the switch implements address learning, forwarding/filtering decisions, and loop avoidance mechanisms as if it were a separate physical bridge. This topic explains how Catalyst switches support VLAN functionality.

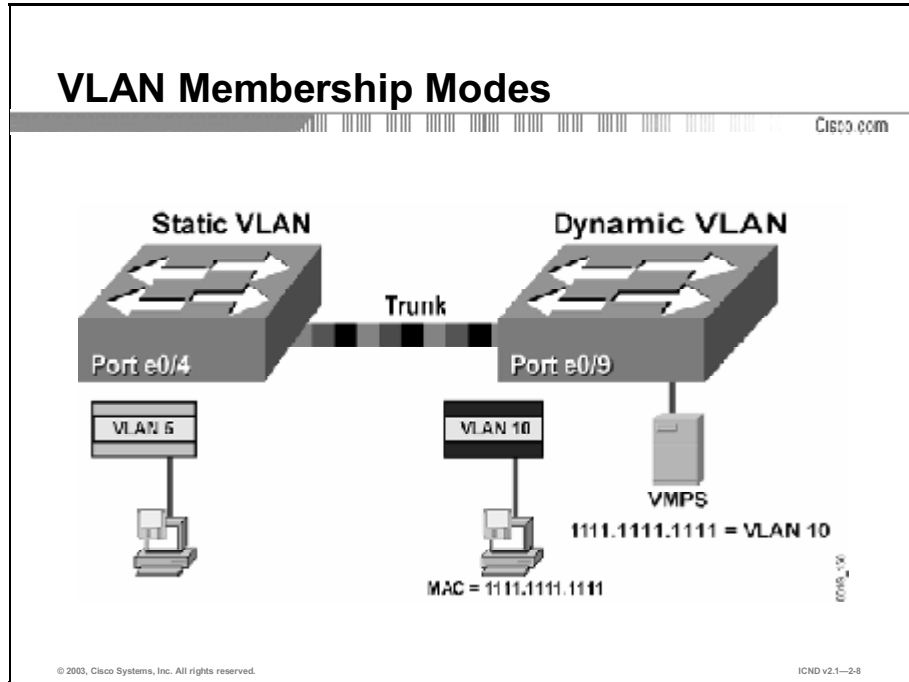


Internally, the Catalyst switch implements VLANs by restricting data forwarding to destination ports in the same VLAN as originating ports. That is, when a frame arrives on a switch port, the Catalyst must retransmit the frame only to ports that belong to the same VLAN. The implication is that a VLAN operating on a Catalyst switch limits transmission of unicast, multicast, and broadcast traffic. Traffic originating from a particular VLAN floods only other ports in that VLAN.

Normally, a port carries traffic only for the single VLAN to which it belongs. For a VLAN to span across multiple switches, a trunk is required to connect two switches. A trunk can carry traffic for multiple VLANs.

VLAN Membership Modes

Ports belonging to a VLAN are configured with a membership mode that determines to which VLAN they belong. Catalyst switches support two VLAN membership modes: static and dynamic. This topic describes the two VLAN membership modes.



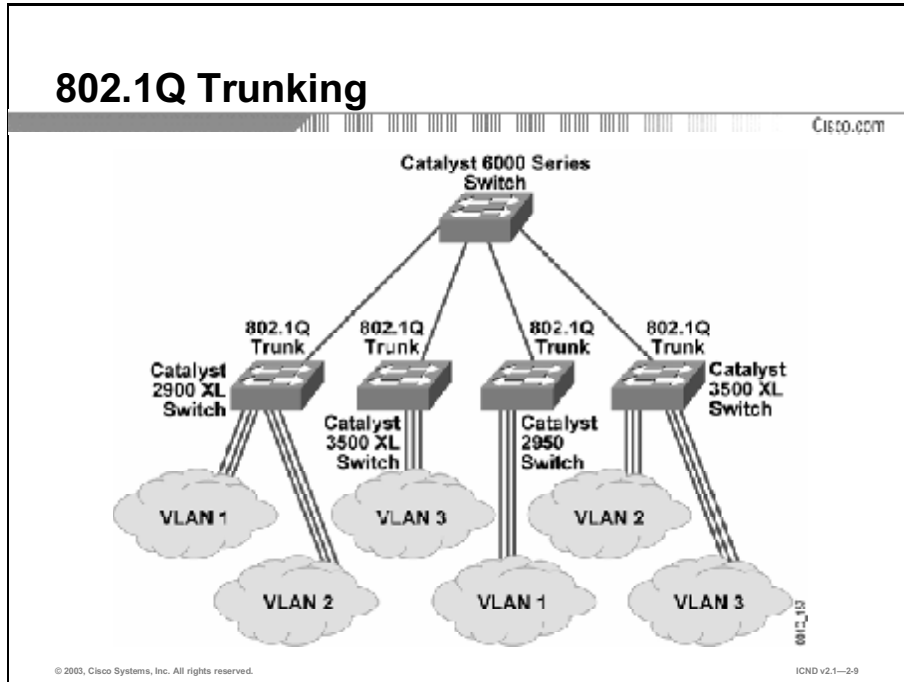
The VLAN membership modes to which Catalyst switch ports can belong are as follows:

- **Static:** Assignment of VLAN to port is configured statically by an administrator.
- **Dynamic:** The Catalyst switches support dynamic VLANs by using a VLAN Management Policy Server (VMPS). The VMPS can be a Catalyst 5000 series switch or an external server; the Catalyst 1900 series or 2950 series cannot operate as the VMPS. The VMPS contains a database that maps MAC addresses to VLAN assignments. When a frame arrives on a dynamic port at the Catalyst access switch, the Catalyst switch queries the VMPS for the VLAN assignment based on the source MAC address of the arriving frame.

A dynamic port can belong to only one VLAN at a time. Multiple hosts can be active on a dynamic port only if they all belong to the same VLAN.

802.1Q Trunking

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers and define VLAN topologies. Cisco supports IEEE 802.1Q for Fast Ethernet and Gigabit Ethernet interfaces. This topic describes the basic functionality provided by 802.1Q trunking.



Trunking is a way to carry traffic from several VLANs over a point-to-point link between the two devices. The two ways in which you can implement Ethernet trunking are as follows:

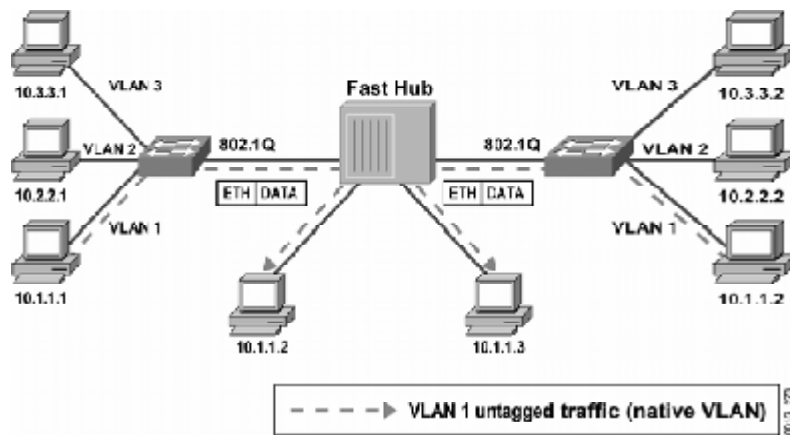
- Inter-Switch Link (ISL), a Cisco proprietary protocol
- 802.1Q, an IEEE standard

IP routing over IEEE 802.1Q extends IP routing capabilities to include support for routing IP frame types in VLAN configurations using the IEEE 802.1Q encapsulation.

Every 802.1Q port is assigned to a trunk. All ports on a trunk are in a native VLAN. Every 802.1Q port is assigned an identifier value that is of its native VLAN ID (default is VLAN 1). All untagged frames are assigned to the LAN specified in the ID parameter.

Importance of Native VLANs

Cisco.com



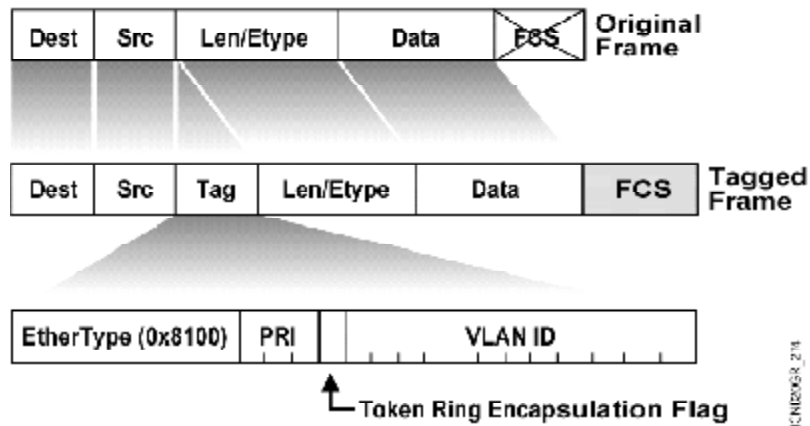
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-10

An 802.1Q trunk and its associated trunk ports have a native VLAN value. 802.1Q does not tag frames for the native VLAN. Therefore, ordinary stations will be able to read the native untagged frames, but not read any other frame because the frames are tagged.

802.1Q Frame

Cisco.com



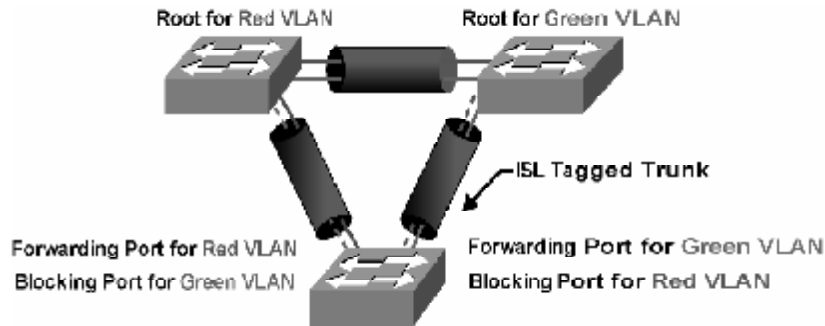
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-11

The figure shows how adding a tag in a frame recomputes the Frame Control Sequence. 802.1p and 802.1Q share the same tag.

Per VLAN Spanning Tree

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-12

The 802.1Q standard is more than just a tagging mechanism. It also defines a unique spanning-tree instance running on the native VLAN for all of the VLANs in the network. An 802.1Q mono spanning tree (MST) network lacks some flexibility compared to a Per VLAN Spanning Tree + (PVST+) network that runs one instance of Spanning Tree Protocol (STP) per VLAN.

Cisco developed PVST+ to allow running several STP instances, even over an 802.1Q network, by using a tunneling mechanism. PVST+ utilizes a Cisco device to connect an MST zone, typically another vendor 802.1Q-based network, to a PVST+ zone, typically a Cisco ISL-based network. There is no specific configuration needed to achieve this. Ideally, a mixed environment should look like the one shown in the figure.

PVST+ provides support for 802.1Q trunks and the mapping of multiple spanning trees to the single spanning tree of 802.1Q switches.

The PVST+ architecture distinguishes three types of regions: a PVST region, a PVST+ region, and an MST region. Each region consists of a homogenous type of switch. You can connect a PVST region to a PVST+ region by connecting two ISL ports. Similarly, you can connect a PVST+ region to an MST region by connecting two 802.1Q ports.

At the boundary between a PVST region and a PVST+ region, the mapping of spanning trees is one-to-one. At the boundary between a MST region and a PVST+ region, the spanning tree in the MST region maps to one PVST in the PVST+ region. The one it maps to is called the *common spanning tree* (CST). The default CST is the PVST of VLAN 1 (native VLAN).

All PVSTs, except for the CST, are tunneled through the MST region. Tunneling means that bridge protocol data units (BPDUs) are flooded through the MST region along the single spanning tree present in the MST region.

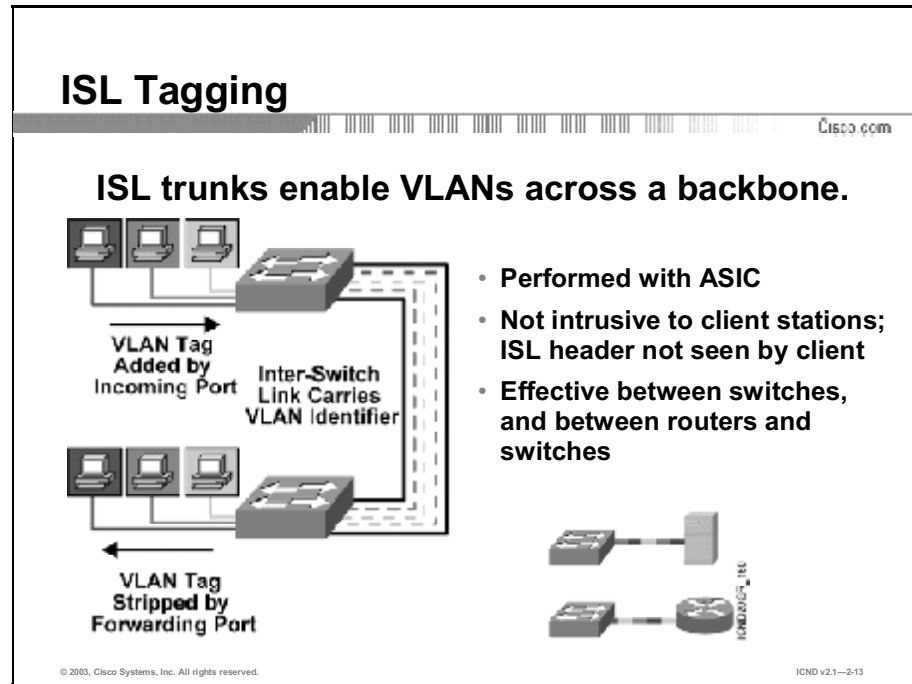
PVST+ networks must be in a tree-like structure for proper STP operation. Providing different STP root switches per VLAN creates a more redundant network.

PVST+ networks provide the following capabilities:

- Allow control of forwarding paths on a subnet basis
- Create flexible design tools for traffic management
- Provide simple techniques for Layer 2 redundancy

ISL Protocol and Encapsulation

Inter-Switch Link (ISL) is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic travels between switches. ISL provides VLAN capabilities while maintaining full wire-speed performance over Fast Ethernet links in full- or half-duplex mode. This topic describes the ISL protocol and encapsulation.



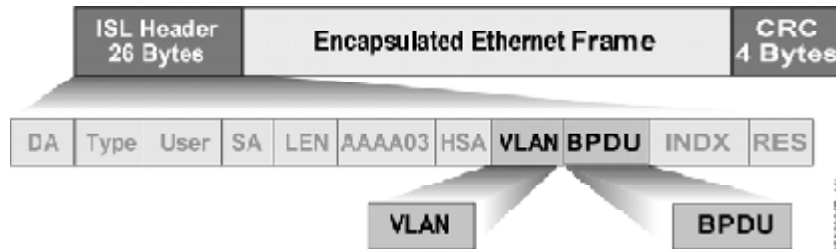
Running a trunk in full-duplex mode is efficient and highly recommended. ISL operates in a point-to-point environment.

The ISL frame tagging that the Catalyst series of switches uses is a low-latency mechanism for multiplexing traffic from multiple VLANs on a single physical path. It has been implemented for connections among switches, routers, and Network Interface Cards (NICs) used on nodes such as servers. To support the ISL feature, each connecting device must be ISL-configured. A router that is ISL-configured is used to allow interVLAN communications. A non-ISL device that receives ISL-encapsulated Ethernet frames may consider them to be protocol errors if the size of the header plus data frame exceeds the maximum transmission unit (MTU) size.

ISL functions at the Open System Interconnection (OSI) Layer 2 reference model by encapsulating a data frame with a new header and cyclic redundancy check (CRC). ISL is protocol-independent, as the data frame may carry any upper-layer protocol. Administrators use ISL to maintain redundant links and load-balance traffic between parallel links using the STP.

ISL Encapsulation

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1-2-14

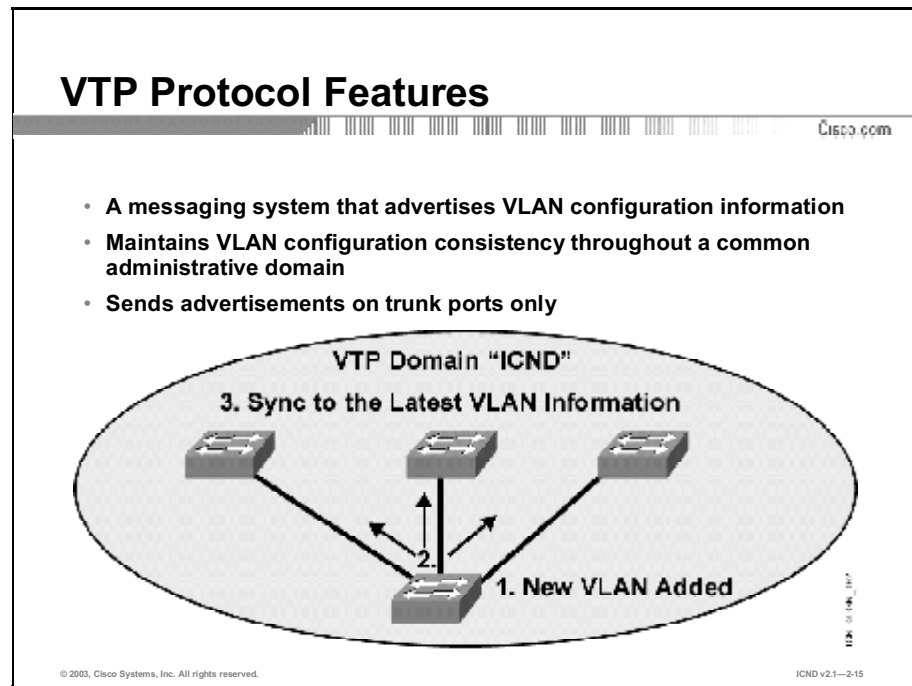
Ports configured as ISL trunks encapsulate each frame with a 26-byte ISL header and a four-byte CRC before sending it out the trunk port. Because ISL technology is implemented in application-specific integrated circuits (ASICs), frames are tagged at wire-speed performance. The number of VLANs supported by a switch depends on the switch hardware.

The ISL frame header contains the following information fields:

- **DA:** 40-bit multicast destination address
- **Type:** Four-bit descriptor of the encapsulated frame types: Ethernet (0000), Token Ring (0001), Fiber Distributed Data Interface (FDDI) (0010), and ATM (0011)
- **User:** Four-bit descriptor used as the type field extension or to define Ethernet priorities; it is a binary value from 0, the lowest priority, to 3, the highest priority
- **SA:** 48-bit source MAC address of the transmitting Catalyst switch
- **LEN:** 16-bit frame-length descriptor minus DA type, user, SA, LEN, and CRC
- **AAAA03:** Standard Subnetwork Access Protocol (SNAP) 802.2 LLC header
- **HSA:** First three bytes of the SA (manufacturer or unique organizational ID)
- **VLAN ID:** 15-bit VLAN ID, only the lower 10 bits are used for 1024 VLANs
- **BPDU:** One-bit descriptor identifying whether the frame is a spanning-tree BPDU; also identifies if the encapsulated frame is a Cisco Discovery Protocol (CDP) frame
- **INDX:** 16-bit descriptor identifying the transmitting port ID; used for diagnostics
- **RES:** 16-bit reserved field used for additional information, such as the FDDI frame control field

VTP Protocol Features

VLAN Trunking Protocol (VTP) is used to distribute and synchronize identifying information about the VLANs that are configured throughout a switched network. VTP allows switched network solutions to scale to large sizes by reducing the manual configuration needs in the network. This topic describes the features that VTP offers to support VLANs.



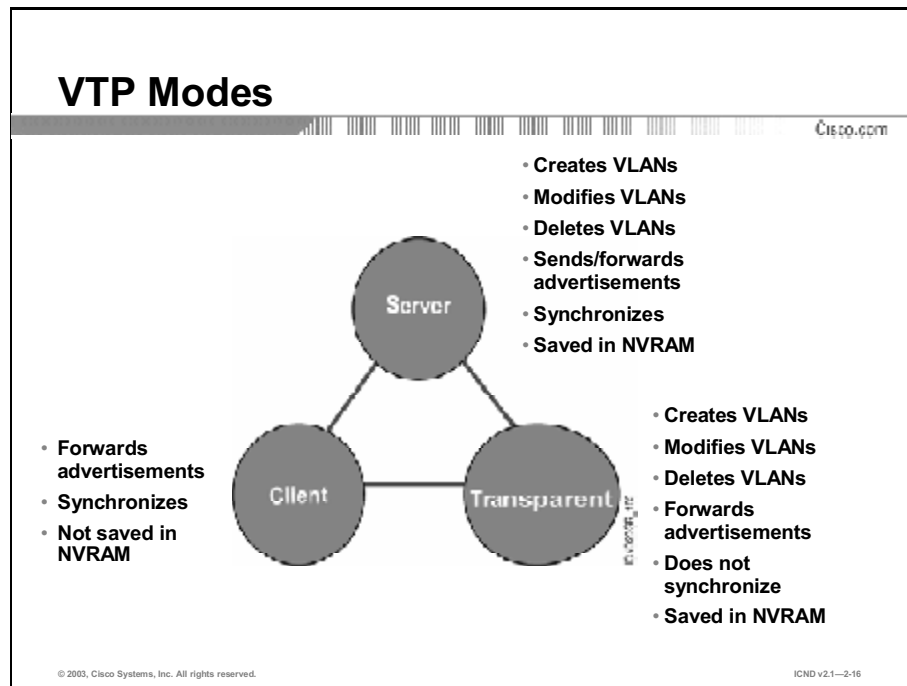
VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the additions, deletions, and name changes of VLANs across networks. VTP minimizes misconfigurations and configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLAN-type specifications.

A VTP domain is one switch or several interconnected switches sharing the same VTP environment. You can only configure a switch to be in one VTP domain.

By default, a Catalyst switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link, or until you configure a management domain. Configurations made to a single VTP server are propagated across links to all connected switches in the network.

VTP Modes, Operation, and Pruning

VTP operates in one of three modes: server mode, client mode, or transparent mode. The default VTP mode is server mode, but VLANs are not propagated over the network until a management domain name is specified or learned. This topic describes the VTP modes, operation, and pruning features.



You can complete different tasks depending on the VTP operation mode. A Catalyst switch operating in the VTP server mode (the default), can create, modify, and delete VLANs and other configuration parameters for the entire VTP domain. In VTP server mode, VLAN configurations are saved in the Catalyst nonvolatile memory. When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP messages are transmitted out all trunk connections, such as ISL.

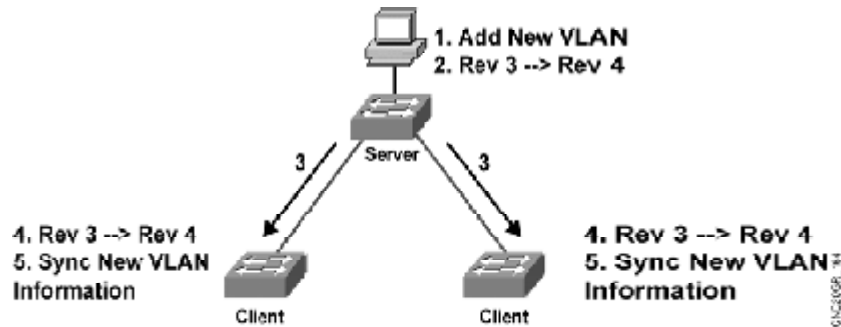
The table describes the features of the VTP client, server, and transparent modes.

VTP Mode	Features
Client	■ Cannot create, change, or delete VLANs. ■ Does not save VLAN configuration in nonvolatile memory. ■ Synchronizes VLAN configuration with latest information received from other switches in the management domain.
Server	■ Synchronizes VLAN configuration with latest information received from other switches in the management domain.
Transparent	■ Does not create VTP advertisements. ■ Does not synchronize its VLAN configuration with information received from other switches in the management domain. ■ Forwards VTP advertisements received from other switches in the same management domain. ■ Can create, delete, and modify VLANs; changes affect the local switch only.

VTP Operation

Cisco.com

- VTP advertisements are sent as multicast frames.
- VTP servers and clients are synchronized to the latest revision number.
- VTP advertisements are sent every 5 minutes or when there is a change.



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-17

VTP advertisements are flooded throughout the management domain. They are sent every 5 minutes or whenever there is a change in VLAN configurations. They are transmitted over a factory default VLAN (VLAN 1) using a multicast frame. A configuration revision number is included in each VTP advertisement; a higher configuration revision number indicates that the VLAN information being advertised is more current than the stored information.

A device that receives VTP advertisements must check various parameters before incorporating the received VLAN information. First, the management domain name and password in the advertisement must match those configured in the local switch. Next, if the configuration revision number indicates that the message was created after the configuration currently in use, the switch incorporates the advertised VLAN information. To reset the configuration revision number on a Catalyst switch, use the **delete vtp** privileged EXEC command.

One of the most critical components of VTP is the configuration revision number. Each time a VTP server modifies its VLAN information, it increments the configuration revision number by one. It then sends out a VTP advertisement with the new configuration revision number. If the configuration revision number being advertised is higher than the number stored on the other switches in the VTP domain, the switches will overwrite their VLAN configurations with the new information being advertised.

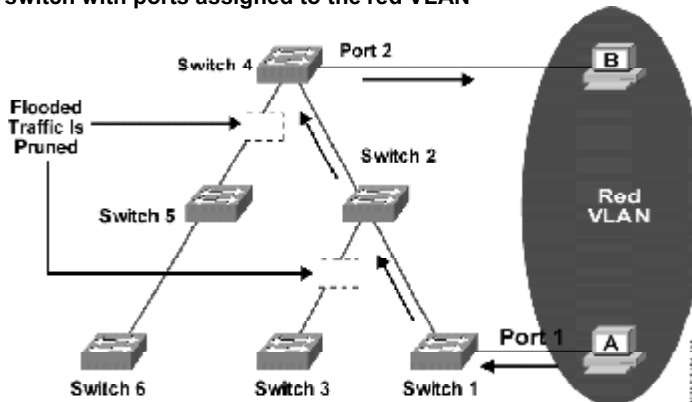
The configuration revision number in VTP transparent mode is always 0.

Note The overwrite process would mean that if the VTP server deleted all VLANs and had the higher revision number, the other devices in the VTP domain would also delete their VLANs.

VTP Pruning

Cisco.com

- Increases available bandwidth by reducing unnecessary flooded traffic
- Example: Station A sends broadcast, and broadcast is flooded only toward any switch with ports assigned to the red VLAN



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-18

VTP pruning uses VLAN advertisements to determine when a trunk connection is flooding traffic needlessly.

By default, a trunk connection carries traffic for all VLANs in the VTP management domain. Commonly, some switches in an enterprise network do not have local ports configured in each VLAN. In the example network in the figure, switches 1 and 4 support ports statically configured in the red VLAN.

VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

The figure shows a switched network with VTP pruning enabled. The broadcast traffic from station A is not forwarded to switches 3, 5, and 6 because traffic for the red VLAN has been pruned on the links indicated on switches 2 and 4.

Pruning can be enabled only on VTP servers, *not* on clients.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **A VLAN permits a group of users to share a common broadcast domain regardless of their physical location in the internetwork. VLANs improve performance and security in switched networks.**
- **A Catalyst switch operates in a network like a traditional bridge. Each VLAN configured on the switch implements address learning, forwarding/filtering decisions, and loop avoidance mechanisms.**
- **Ports belonging to a VLAN are configured with a membership mode that determines to which VLAN they belong. Catalyst switches support two VLAN membership modes: static and dynamic.**
- **The IEEE 802.1Q protocol is used to transport frames for multiple VLANs between switches and routers, and for defining VLAN topologies.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-19

Summary (Cont.)

Cisco.com

- **ISL is a Cisco proprietary protocol to transport multiple VLANs between switches and routers. ISL provides VLAN tagging capabilities while maintaining full wire-speed performance.**
- **VTP is a protocol used to distribute and synchronize identifying information about VLANs configured throughout a switched network. VTP allows switched network solutions to scale to large sizes by reducing the manual configuration required on each switch in the network.**
- **VTP operates in one of three modes: server, client, or transparent. The default VTP mode is server mode, but VLANs are not propagated over the network until a management domain name is specified or learned.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-20

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which four statements describe a VLAN? (Choose four.)
- A) It is hard to add new users.
 - B) It can span multiple switches.
 - C) It is a common collision domain.
 - D) It is a common broadcast domain.
 - E) It can span multiple ports of a switch.
 - F) It can be used to group users, regardless of their physical location.
- Q2) What is the main benefit of a VLAN?
- A) better security
 - B) earlier switch administration
 - C) improved network performance
 - D) better Spanning Tree Protocol implementation
- Q3) When a frame arrives on a switch port on a Catalyst switch, what does the switch do with it?
- A) It floods broadcast traffic to all VLANs.
 - B) It discards frames that are addressed to routed networks.
 - C) It restricts data forwarding to destination ports in the same VLAN as the originating port.
 - D) It retransmits the frame to all ports that belong to the same VLAN, including the received port.
- Q4) Each VLAN configured on a switch implements address learning, forwarding and filtering decisions, and loop-avoidance mechanisms as if it were a separate ____.
- A) physical hub
 - B) physical router
 - C) physical bridge
 - D) physical switch
- Q5) Which statement describes VLAN membership on a Catalyst switch?
- A) requires the use of VTP
 - B) requires the use of VSM software
 - C) requires the use of a VMPS server
 - D) allows ports to belong to more than one VLAN

- Q6) How many VLANs can a dynamic port belong to on a Catalyst switch?
- A) 1
 - B) 2
 - C) 3
 - D) 4
- Q7) Which two trunking methods does Cisco use to define VLAN topologies? (Choose two.)
- A) IP trunking
 - B) ISL trunking
 - C) 802.11 trunking
 - D) 802.1Q trunking
 - E) Fast Ethernet trunking
- Q8) What is the primary benefit of implementing Per VLAN Spanning Tree?
- A) increases security
 - B) reduces collisions
 - C) eases network administration
 - D) increases network redundancy
- Q9) Which three statements describe the characteristics of ISL? (Choose three.)
- A) ISL is an IEEE protocol.
 - B) ISL is a Cisco proprietary protocol.
 - C) ISL is used to interconnect switches.
 - D) ISL can be used to connect switches to servers.
 - E) ISL operates at the network layer, allowing it to encapsulate Layer 2 frames.
- Q10) What components does an ISL frame include?
- A) 30 bytes of header
 - B) 26 bytes of header and 4 bytes of trailer
 - C) 30 bytes of header and 2 bytes of trailer
 - D) 44 bytes of header and 4 bytes of trailer
- Q11) Which two statements are true about VTP? (Choose two.)
- A) VTP is a data-link layer protocol.
 - B) There are two VTP modes: server and client.
 - C) VTP advertisements are sent on all switch ports.
 - D) A switch can be in multiple VTP domains, but only in one per port.
 - E) VTP is used to distribute and synchronize identifying information about VLANs.

- Q12) At what layer of the OSI reference model does VTP operate?
- A) Layer 1
 - B) Layer 2
 - C) Layer 3
 - D) Layer 4
- Q13) Which two statements about configuring a VTP domain name on a Catalyst switch are true? (Choose two.)
- A) You must manually configure the VTP domain name.
 - B) The VTP domain name is required before VTP will function.
 - C) A switch can learn the VTP domain name from another switch.
 - D) Configuring the VTP domain name requires that you configure a VTP password.
- Q14) What is the default VTP mode for a Catalyst switch?
- A) client
 - B) server
 - C) trunking
 - D) full-duplex

Quiz Answer Key

- Q1) B, D, E, F
Relates to: Defining a VLAN
- Q2) C
Relates to: Defining a VLAN
- Q3) C
Relates to: VLAN Operation
- Q4) C
Relates to: VLAN Operation
- Q5) C
Relates to: VLAN Membership Modes
- Q6) A
Relates to: VLAN Membership Modes
- Q7) B, D
Relates to: 802.1Q Trunking
- Q8) D
Relates to: 802.1Q Trunking
- Q9) B, C, D
Relates to: ISL Protocol and Encapsulation
- Q10) B
Relates to: ISL Protocol and Encapsulation
- Q11) A, E
Relates to: VTP Protocol Features
- Q12) B
Relates to: VTP Protocol Features
- Q13) B, C
Relates to: VTP Modes, Operation, and Pruning
- Q14) B
Relates to: VTP Modes, Operation, and Pruning

Configuring VLANs

Overview

To configure a virtual LAN (VLAN), you will complete the following tasks:

1. Configure VLAN Trunking Protocol (VTP) mode on all switches, ensuring that only one is the server.
2. On all switches, configure trunks to the appropriate neighbors.
3. On the VTP server switch, configure the VLANs in the network.
4. On each switch, assign ports to their appropriate VLANs.
5. On each switch, configure the interface for the management VLAN (VLAN 1) and assign the appropriate IP address.

This lesson explains how to complete the VLAN configuration tasks.

Relevance

You will configure VLANs on large switched networks. Understanding how to configure them properly is an important task for you to learn.

Objectives

Upon completing this lesson, you will be able to:

- Use Cisco IOS commands to configure VLANs, VTP, IEEE 802.1Q trunking, and Inter-Switch Link trunking, given a functioning access layer switch
- Execute an add, move, or change on an access layer switch, given a new network requirement
- Use **show** commands to identify anomalies in VLAN, VTP, IEEE 802.1Q trunking, Inter-Switch Link trunking, and spanning-tree operation within a VLAN, given an operational access layer switch
- Use **debug** commands to identify events and anomalies in VLAN, VTP, IEEE 802.1Q trunking, Inter-Switch Link trunking, and spanning-tree operation, given an operational access layer switch

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

Outline

The lesson includes these topics:

- Overview
- Configuring VTP
- Configuring 802.1Q Trunking
- Configuring ISL Trunking
- Configuring a VLAN
- Assigning Ports to a VLAN
- Verifying the VLAN Configuration
- Executing Adds, Moves, and Changes for VLANs
- Troubleshooting VLANs
- Summary
- Quiz

Configuring VTP

Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) in your network. With VTP, you can make configuration changes on one or more switches and those changes are automatically communicated to all other switches in the network. This topic explains how to configure VTP.

VTP Configuration Guidelines



- **VTP domain name**
- **VTP mode (server/client/transparent) VTP server mode is the default**
- **VTP pruning**
- **VTP password**
- **VTP trap**

Use caution when adding a new switch to an existing domain.
Add a new switch in client mode to prevent the new switch from propagating incorrect VLAN information.

Use the delete vtp command to reset the VTP revision number.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—2-4

Default VTP configuration values depend on the switch model and the software version. For example, the default values for the Catalyst 1900 series and 2950 series switches are as follows:

- **VTP domain name:** None
- **VTP mode:** Server
- **VTP password:** None
- **VTP pruning:** Enabled (Catalyst 1900 series), Disabled (Catalyst 2950 series)
- **VTP trap:** Enabled (Catalyst 1900 series), Disabled (Catalyst 2950 series)

The VTP domain name can be specified or learned. By default, the domain name is not set.

You can set a password for the VTP management domain. The password should be the same for all switches in the domain. If you configure a VTP password, VTP does not function properly unless you assign the same password to each switch in the domain.

VTP pruning eligibility is one VLAN parameter that the VTP protocol advertises. Enabling or disabling VTP pruning on a VTP server propagates the change throughout the management domain.

Creating a VTP Domain

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900(config)#vtp [server | transparent | client] [domain
domain-name] [trap {enable | disable}] [password password]
[pruning {enable | disable}]
```

```
wg_sw_1900#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
wg_sw_1900(config)#vtp transparent
wg_sw_1900(config)#vtp domain switchlab
```

Catalyst 2950 Series

```
wg_sw_2950#vlan database
wg_sw_2950(vlan)#vtp [ server | client | transparent ]
wg_sw_2950(vlan)#vtp domain domain-name
wg_sw_2950(vlan)#vtp password password
wg_sw_2950(vlan)#vtp pruning
wg_sw_2950(vlan)#snmp-server enable traps vtp
wg_sw_2950(vlan)#exit
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-5

On the Catalyst 1900 series, use the **vtp** global configuration command to specify the operating mode, domain name, password, generation of traps, and pruning capabilities of VTP.

The Catalyst 2950 series also uses the **vtp** command, but you must enter each parameter on a separate line in VLAN configuration mode. Use the **vlan database** command in privileged EXEC mode to start VLAN configuration mode. Then use the **exit** command to return to privileged EXEC mode.

Note The domain name and password are case sensitive. A domain name cannot be removed after it is assigned; it can only be *reassigned*.

VTP Configuration Example

Cisco.com

```
wg_sw_1900(config)#vtp transparent
wg_sw_1900(config)#vtp domain switchlab pruning enable
wg_sw_1900(config)#exit
wg_sw_1900#show vtp
VTP version: 1
  Configuration revision: 4
  Maximum VLANs supported locally: 1005
  Number of existing VLANs: 6
  VTP domain name       : switchlab
  VTP password          :
  VTP operating mode    : Transparent
  VTP pruning mode      : Enabled
  VTP traps generation  : Enabled
  Configuration last modified by: 0.0.0.0 at 00-00-0000
00:00:00
wg_sw_1900#config terminal
wg_sw_1900(config)#interface f0/26
wg_sw_1900(config-if)#trunk on desirable
wg_sw_1900(config-if)#exit
wg_sw_1900(config)#exit
wg_sw_1900#show trunk A
DISL state: On, Trunking: On, Encapsulation type: ISL
```

© 2003, Cisco Systems, Inc. All rights reserved.

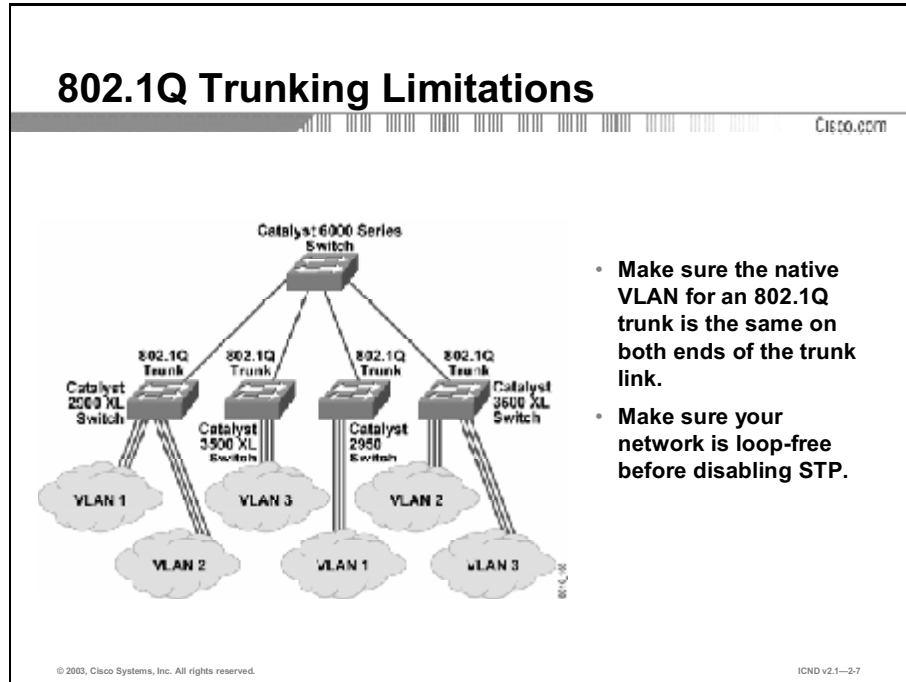
ICND v2.1—2-6

The figure demonstrates the sequence of commands that you would enter to configure VTP and trunking on a Catalyst 1900 series switch with the following characteristics:

- Switch is transparent in the VTP domain.
- VTP domain name is “switchlab.”
- Pruning is enabled.
- Trunk is on port f0/26.
- Trunking is in desirable negotiation.

Configuring 802.1Q Trunking

You will configure IEEE 802.1Q to carry traffic for multiple VLANs over a single link on a multivendor network. This topic explains how to configure IEEE 802.1Q trunking on a Catalyst 2950 series switch.



IEEE 802.1Q trunks impose the following limitations on the trunking strategy for a network:

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Make sure your network is loop-free before disabling Spanning Tree Protocol (STP).

IEEE 802.1Q trunking interacts with other switch features as described in the table.

Switch Feature	Trunk Port Interaction
Secure ports	A trunk port cannot be a secure port.
Port grouping	802.1Q trunks can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting you entered to all ports in the group. The settings include the following: ■ Allowed-VLAN list ■ STP path cost for each VLAN ■ STP port priority for each VLAN ■ STP PortFast setting ■ Trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks

Configuring 802.1Q Trunking

Cisco.com

```
wg_sw_a(config-if)#switchport mode trunk
```

- **Configures the port as a VLAN trunk**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-8

Use the **switchport mode** interface configuration command to set a Fast Ethernet or Gigabit Ethernet port to trunk mode. The Catalyst 1900 series and 2950 series switches support the Dynamic Trunk Protocol (DTP), which manages automatic trunk negotiation.

The **switchport mode** command has five options, as follows:

- **trunk:** Configures the port into permanent 802.1Q trunk mode and negotiates with the connected device to convert the link to trunk mode.
- **access:** Disables port trunk mode and negotiates with the connected device to convert the link to nontrunk.
- **dynamic desirable:** Triggers the port to negotiate the link from nontrunk to trunk mode. The port negotiates to a trunk port if the connected device is either in the *trunk*, *desirable*, or *auto* state. Otherwise, the port becomes a nontrunk port, which is the default mode for all Ethernet interfaces.
- **dynamic auto:** Enables a port to become a trunk only if the connected device has the state set to *trunk* or *desirable*. Otherwise, the port becomes a nontrunk port.
- **nonnegotiate:** Configures the port to permanent 802.1Q trunk mode and no negotiation takes place with the partner.

Beginning in privileged EXEC mode, follow these steps to configure a port as an 802.1Q trunk port:

Step	Action	Notes
1.	Enter the interface configuration mode and the port to be configured for trunking. <code>wg_sw_a(config)#interface interface</code>	After the interface configuration is entered, the CLI ¹ prompt will change from <code>(config)#</code> to <code>(config-if)#</code> .
2.	Configure the port as a VLAN trunk. <code>wg_sw_a(config-if)#switchport mode trunk</code>	Enable trunking on the selected interface.

¹CLI = command-line interface

Note	Catalyst 2950 series switches only support 802.1Q encapsulation, which is configured automatically when trunking is enabled on the interface by using the switchport mode trunk command.

Configuring ISL Trunking

Inter-Switch Link (ISL) operates in a point-to-point environment to carry traffic for multiple VLANs over a single link. This topic explains how to configure ISL trunking on a Catalyst 1900 series switch.

Configuring ISL Trunking

Cisco.com

```
wg_sw_1900(config-if)#trunk [on | off | desirable | auto |
nonnegotiate]
```

- **on** = Set trunk on and negotiate with other side
- **off** = Set trunk off and negotiate with other side
- **desirable** = Negotiate with other side; trunk on if other side is on, desirable, or auto
- **auto** = Will be a trunk only if the other side is on or desirable
- **nonnegotiate** = Set trunk on and will not negotiate

```
wg_sw_1900#conf terminal
Enter configuration commands, one per line. End with CNTL/Z
wg_sw_1900(config)#interface f0/26
wg_sw_1900(config-if)#trunk on
```

↑
First Trunk Port (Port A)

- **Note:** The Catalyst 1900 series supports ISL encapsulation only.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—2-9

Use the **trunk** interface configuration command to set a Catalyst 1900 series Fast Ethernet port to trunk mode. The Catalyst 1900 series and 2950 series switches support the DTP, which manages automatic trunk negotiation.

The **trunk** command has five options, as follows:

- **on:** Configures the port into permanent ISL trunk mode and negotiates with the connected device to convert the link to trunk mode.
- **off:** Disables port trunk mode and negotiates with the connected device to convert the link to nontrunk.
- **desirable:** Triggers the port to negotiate the link from nontrunk to trunk mode. The port negotiates to a trunk port if the connected device is either in the on, desirable, or auto state. Otherwise, the port becomes a nontrunk port.
- **auto:** Enables a port to become a trunk only if the connected device has the state set to on or desirable.
- **nonnegotiate:** Configures the port to permanent ISL trunk mode and no negotiation takes place with the partner.

Note Catalyst 1900 series switches support ISL encapsulation only, which is configured automatically when trunking is enabled on the interface by using the **trunk** command.

Configuring a VLAN

Most Catalyst desktop switches support a maximum of 64 active VLANs. The Catalyst 1900 series supports 1024 VLANs with the Enterprise Edition software. Depending on the model, the 2950 series can support up to 250 VLANs. This topic explains how to create new VLANs and modify VLAN names.

VLAN Configuration Guidelines

CISCO.COM

- **Maximum number of VLANs is switch-dependent.**
- **Catalyst desktop switches support 64 VLANs with a separate spanning tree per VLAN.**
- **VLAN 1 is the factory default Ethernet VLAN.**
- **CDP and VTP advertisements are sent on VLAN 1.**
- **The Catalyst switch IP address is in the management VLAN (VLAN 1 by default).**
- **To add or delete VLANs, the switch must be in VTP server or transparent mode.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-10

Catalyst switches have a factory default configuration where various default VLANs are preconfigured to support various media and protocol types. The default Ethernet VLAN is VLAN 1. Cisco Discovery Protocol (CDP) and VTP advertisements are sent on VLAN 1.

For you to be able to communicate with the Catalyst switch remotely for management purposes, the switch must have an IP address. This IP address must be in the management VLAN, which by default is VLAN 1. Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode.

Adding a VLAN

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900(config)#vlan vlan# [name vlan-name]
```

```
wg_sw_1900#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
wg_sw_1900(config)#vlan 9 name switchlab2
```

Catalyst 2950 Series

```
wg_sw_2950#vlan database
wg_sw_2950(vlan)#vlan vlan# [name vlan-name]
```

```
wg_sw_2950#vlan database
wg_sw_2950(vlan)#vlan 9 name switchlab2
wg_sw_2950(vlan)#exit
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-11

Before you create VLANs, you must decide whether or not to use VTP to maintain global VLAN configuration information for your network.

To allow VLANs to span across multiple switches, you must configure trunks to interconnect the switches.

By default, a switch is in VTP server mode so that you can add, change, or delete VLANs. If the switch is set to VTP client mode, you cannot add, change, or delete VLANs.

For the Catalyst 1900 series switch, use the **vlan** global configuration command to configure a new VLAN. For the Catalyst 2950 series switch, use the **vlan** command from VLAN configuration mode.

Modifying a VLAN Name

Cisco.com

```
wg_sw_a(config)#vlan vlan# name vlan-name
```

```
wg_sw_a#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
wg_sw_a(config)#vlan 9 name switchlab90
```

```
wg_sw_a#show vlan 9
```

VLAN Name	Status	Ports
9	switchlab90	Enabled

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-12

To modify an existing VLAN name or number, use the same command syntax used to add a VLAN. In the Catalyst 1900 series switch example shown in the figure, the VLAN name for VLAN 9 is changed to switchlab90.

Each VLAN has a unique, four-digit ID that is a number from 0001 to 1005. To add a VLAN to the VLAN database, assign a number and name to the VLAN. VLAN 1 (including VLAN1002, VLAN1003, VLAN1004, and VLAN1005) is the factory default VLAN.

To add an Ethernet VLAN, you must specify at least a VLAN number. If no VLAN name is entered for the VLAN, the default is to append the VLAN number to the word **vlan**. For example, VLAN0004 could be a default name for VLAN 4 if no name is specified.

Assigning Ports to a VLAN

After creating a VLAN, you can statically assign a port or a number of ports to that VLAN. A port can belong to only one VLAN at a time. This topic explains how to assign switch ports to a VLAN.

Assigning Switch Ports to a VLAN

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900(config-if)#vlan-membership {static {vlan#} | dynamic}
```

```
wg_sw_1900#conf terminal
Enter configuration commands, one per line. End with CNTL/Z
wg_sw_1900(config)#interface ethernet 0/8
wg_sw_1900(config-if)#vlan-membership static 9
```

Catalyst 2950 Series

```
wg_sw_2950(config-if)#switchport access vlan vlan#
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—2-13

VLAN membership on the switch ports is assigned manually on a port-by-port basis. When you assign switch ports to VLANs using this method, it is known as port-based, or static, VLAN membership.

On a Catalyst 1900 series switch, configure the VLAN port assignment from the interface configuration mode using the **vlan-membership** command. Use the **static** *vlan#* option to set static membership. Use the **dynamic** option to have the VLAN dynamically assigned.

On a Catalyst 2950 series switch, configure the *vlan#* port assignment from the interface configuration mode using the **switchport access** command. Use the **vlan** *vlan#* option to specify the default VLAN which is used if the interface stops trunking.

By default, all ports are members of VLAN 1.

Verifying the VLAN Configuration

You can verify the VLAN configuration using the **show** commands. This topic describes the output for each **show** command to verify the configuration of VTP, trunking, VLANs, port membership, and spanning tree for a VLAN on the Catalyst 1900 and 2950 series switches.

Verifying the VTP Configuration for the Catalyst 1900 Series

CISCO.COM

```
wg_sw_1900#show vtp
```

```
wg_sw_1900#show vtp
VTP version: 1
Configuration revision: 4
Maximum VLANs supported locally: 1005
Number of existing VLANs: 6
VTP domain name       : switchlab
VTP password          :
VTP operating mode     : Transparent
VTP pruning mode      : Enabled
VTP traps generation   : Enabled
Configuration last modified by: 10.1.1.40 at 00-00-0000 00:00:00
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-14

On a Catalyst 1900 series switch, use the **show vtp** privileged EXEC command to verify a recent configuration change, or to view the VTP configuration information.

Also displayed is the IP address of the device that last modified the configuration, as well as a time stamp indicating when the modification was made. VTP has two versions: VTP version 1 supports only Ethernet; VTP version 2 supports Ethernet and Token Ring. The VTP version must be the same for all switches in the management domain.

Verifying the VTP Configuration for the Catalyst 2950 Series

Cisco.com

```
wg_sw_2950#show vtp status
```

```
wg_sw_2950#show vtp status
VTP Version                : 2    <--- Indicates v2-capable
Configuration Revision      : 4
Maximum VLANs supported locally : 68
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             : switchlab
VTP Pruning Mode            : Enabled
VTP V2 Mode                 : Disabled <--- Indicates v2 disabled; v1 set
VTP Traps Generation        : Disabled <--- Catalyst 2950 default
MD5 digest                  : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
Configuration last modified by 10.1.1.40 at 5-4-02 22:25:
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-15

On a Catalyst 2950 series switch, use the **show vtp status** command to verify a recent configuration change or to view the VTP configuration information.

Example output for a Catalyst 2950 series switch is as follows:

```
wg_sw_2950#show vtp status
VTP Version                : 2    <--- Indicates v2-capable
Configuration Revision      : 4
Maximum VLANs supported locally : 68
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             : switchlab
VTP Pruning Mode            : Enabled
VTP V2 Mode                 : Disabled <--- Indicates v2
disabled; v1 set
VTP Traps Generation        : Disabled <--- Catalyst 2950
default
MD5 digest                  : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1
0x03
Configuration last modified by 10.1.1.40 at 5-4-02 22:25:
```

Verifying a Trunk

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#show trunk [A | B]
```

```
wg_sw_1900#show trunk a
DISL state: On, Trunking: On, Encapsulation type: ISL
```

Catalyst 2950 Series

```
wg_sw_2950#show interface interface switchport
```

```
wg_sw_2950#show interface fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
. . .
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-16

To verify a trunk configuration on a Catalyst 1900 series switch, use the **show trunk** privileged EXEC command to display the trunk parameters. You must specify the specific trunk to display, which may be one of the following:

- Port A = FastEthernet0/26
- Port B = FastEthernet0/27

To verify a trunk configuration on a Catalyst 2950 series switch, use the **show interface interface switchport** privileged EXEC command to display the trunk parameters. The Catalyst 2950 series switch supports trunking on each of its Fast Ethernet and Gigabit Ethernet ports.

Verifying a VLAN

Cisco.com

Catalyst 1900 Series

```
wg_sw_1900#show vlan [vlan#]
```

```
wg_sw_1900#show vlan 9
```

VLAN Name		Status	Ports	
9 switchlab2		Enabled		
VLAN Type		SAID	MTU	Parent RingNo BridgeNo Stp Trans1 Trans2
9 Ethernet		100009	1500	0 1 1 Unkn 0 0

Catalyst 2950 Series

```
wg_sw_2950#show vlan [id vlan#]
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-17

After the VLAN is configured, you should validate the parameters for that VLAN.

On the Catalyst 1900 series switch, verify the parameters that are configured for a particular VLAN using the **show vlan vlan#** privileged EXEC command.

On the Catalyst 2950 series switch, use the **show vlan id vlan#** privileged EXEC command to display information about a particular VLAN.

On either switch, use the **show vlan** command to display information on all configured VLANs.

The **show** command displays the switch ports assigned to each VLAN. Other VLAN parameters displayed include the type (the default is Ethernet), SAID (Security Association Identifier, used for Fiber Distributed Data Interface [FDDI] trunk), maximum transmission unit (MTU [the default is 1500 for Ethernet VLAN]), STP (the Catalyst 1900 series switch supports only the 802.1d STP standard), and other parameters used for Token Ring or FDDI VLANs.

Verifying VLAN Membership on a Catalyst 1900 Series

Cisco.com

```
wg_sw_1900#show vlan-membership
```

```
wg_sw_1900#show vlan-membership
```

Port	VLAN	Membership Type	Port	VLAN	Membership Type
1	5	Static	13	1	Static
2	1	Static	14	1	Static
3	1	Static	15	1	Static
4	1	Static	16	1	Static
5	1	Static	17	1	Static
6	1	Static	18	1	Static
7	1	Static	19	1	Static
8	9	Static	20	1	Static

Note: port 1=e0/1, port 2=e0/2

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-18

On the Catalyst 1900 series switch, use the **show vlan-membership** privileged EXEC command to display the VLAN assignment and membership type for all switch ports.

Port 1 refers to Ethernet 0/1, port 2 refers to Ethernet 0/2, and so on.

Verifying VLAN Membership on a Catalyst 2950 Series

Cisco.com

```
wg_sw_2950#show vlan brief
```

```
wg_sw_2950#show vlan brief
VLAN    Name                Status    Ports
-----
1        default             active    Fa0/4, Fa0/5, Fa0/6, Fa0/7,
                           Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                           Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                           Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                           Fa0/20, Fa0/21
5        VLAN5               active    Fa0/3
9        VLAN9               active    Fa0/22, Fa0/23
1002     fddi-default         active
1003     token-ring-default   active
1004     fddinet-default      active
1005     trnet-default        active
```

```
wg_sw_2950#show interfaces interface switchport
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-19

On the Catalyst 2950 series switch, use the **show vlan brief** privileged EXEC command to display the VLAN assignment and membership type for all switch ports. Alternatively, use the **show interfaces interface switchport** privileged EXEC command to display the VLAN information for a particular interface.

Verifying STP for a VLAN

Cisco.com

Catalyst 1900 Series

wg_sw_1900#show spantree [vlan#]

```
wg_sw_1900#show spantree 1

VLAN1 is executing the IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 0050.F037.DA00
Configured hello time 2, max age 20, forward delay 15
Current root has priority 0, address 00D0.588F.B600
Root port is FastEthernet 0/26, cost of root path is 10
Topology change flag not set, detected flag not set
Topology changes 53, last topology change occurred 0d00h17m14s ago
Times: hold 1, topology change 8960
      hello 2, max age 20, forward delay 15
Timers: hello 2, topology change 35, notification 2
Port Ethernet 0/1 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 0, address 00D0.588F.B600
Designated bridge has priority 32768, address 0050.F037.DA00
Designated port is Ethernet 0/1, path cost 10
Timers: message age 20, forward delay 15, hold 1
```

Catalyst 2950 Series

wg_sw_2950#show spanning-tree vlan [vlan#]

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-20

On the Catalyst 1900 series switch, use the **show spantree** privileged EXEC command to display the Spanning Tree Protocol (STP) configuration status for a particular VLAN. A quick and simple way to understand your network and to see which features you have enabled on each switch is to issue the **show spantree summary** command on each switch. The following information is provided:

- VLANs running STP
- Number of ports in each VLAN
- Ports on the switch that are blocking and on which VLANs they are blocking

On the Catalyst 2950 series switch, use the **show spanning-tree vlan** privileged EXEC command to display the STP configuration status for a particular VLAN.

In the example, spanning-tree information for VLAN 1 on a Catalyst 1900 series switch is shown, including the following:

- Port e0/1 is in the forwarding state for VLAN 1
- The root bridge for VLAN 1 has a bridge priority of 0 with a MAC address of 00D0.588F.B600
- The switch is running the IEEE 802.1d STP

Recall that a Catalyst switch can support a separate spanning tree per VLAN, allowing for load balancing between switches. For example, one switch can be the root for VLAN 1, while another switch can be the root for VLAN 2. (This idea is explained further in the *Building Cisco Multilayer Switched Networks* [BCMSN] course.)

Executing Adds, Moves, and Changes for VLANs

As network topologies, business requirements, and individual assignments change, VLAN requirements also change. This topic describes how to add, move, and change VLANs.

Executing Adds, Moves, and Changes for VLANs



```
wg_sw_a(config)#vlan database
```

- Enters the vlan database privileged EXEC command to access VLAN configuration mode
- Writes VLAN adds, moves, and changes to the vlan.dat file

```
wg_sw_a(config)#vlan vlan-id mtu mtu-size
```

- Identifies a VLAN and changes the MTU size

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—221

To add, change, or delete VLANs, the switch must be in VTP server or transparent mode. When you make VLAN changes from a switch that is in VTP server mode, the change is automatically propagated to other switches in the VTP domain. VLAN changes made from a switch in VTP transparent mode impacts the local switch only; changes are not propagated to the domain.

Adding VLANs and Port Membership

After a new VLAN is created, be sure to make the necessary changes to VLAN port assignments.

Separate VLANs typically imply separate IP networks. Be sure to plan the new IP addressing scheme and its deployment to stations prior to moving users to the new VLAN. Separate VLANs will also require interVLAN routing to permit users in the new VLAN to communicate with other VLANs. This includes setting up the appropriate IP parameters and services including default gateway and Dynamic Host Configuration Protocol (DHCP).

Changing VLANs and Port Membership

To modify VLAN attributes, such as VLAN name, use the **vlan** command. For the Catalyst 1900 series switch, this command is entered from global configuration mode. For the Catalyst 2950 series switch, this command is entered from VLAN configuration mode. (Use the **vlan database** command to enter VLAN configuration mode; use **exit** to leave this mode.)

Note	The VLAN number cannot be changed. To use a different VLAN number, create the new VLAN using the new number, then reassign all ports to this VLAN.

To move a port into a different VLAN, use the same commands used to make the original assignments. For the Catalyst 1900 series switch, use the **vlan-membership** command to configure or reconfigure the VLAN port assignment. For the Catalyst 2950 series switch, use the **switchport access** command to perform this function. These commands are entered from interface configuration mode.

There is no need to first remove a port from a VLAN to make this change. After a port is reassigned to a new VLAN, it is automatically removed from its previous VLAN.

Deleting VLANs and Port Membership

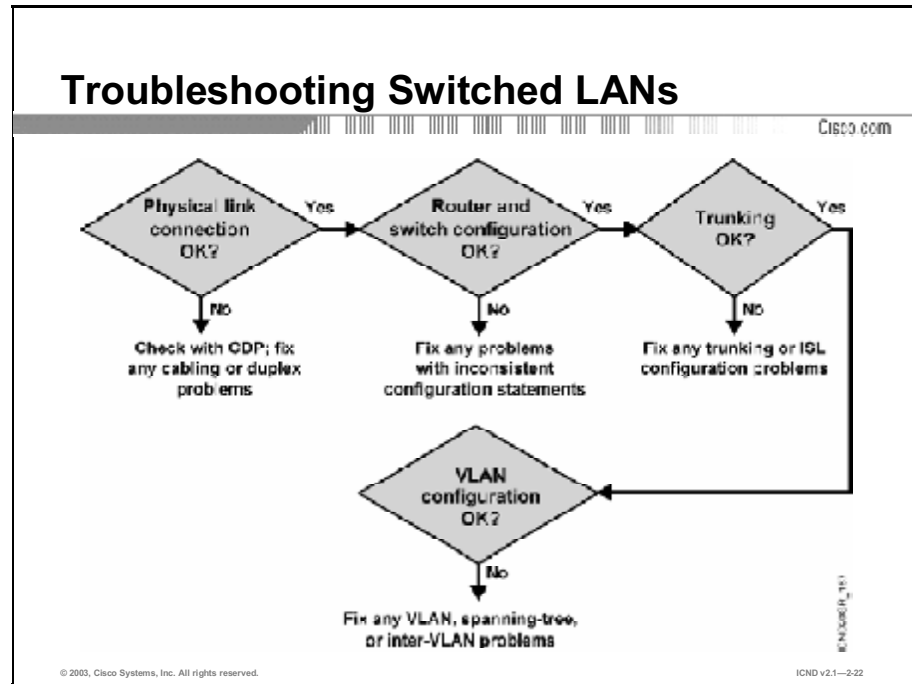
When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted on that specific switch only. Use the **no vlan *vlan-id*** command to remove a VLAN. For the Catalyst 1900 series switch, this command is entered from global configuration mode. For the Catalyst 2950 series switch, this command is entered from VLAN configuration mode.

Note	Before deleting a VLAN, be sure to first reassign all member ports to a different VLAN. Any ports that are not moved to an active VLAN will be unable to communicate with other stations.

To reassign a port to the default VLAN (VLAN 1), use the **no vlan-membership** command for the Catalyst 1900 series, or the **no switchport access vlan** command for the Catalyst 2950 series, in interface configuration mode.

Troubleshooting VLANs

Misconfiguration of a VLAN is one of the most common errors in switched networks. This topic describes the most common misconfiguration errors and suggests solutions to help you troubleshoot your switched network.



The table shows high-level VLAN problems that can occur with a router or switch. The problem facts or symptoms and the possibilities and action plans may help you identify and solve the problems.

Problem Facts	Possible Problems and Action Plans
Performance on the VLAN is slow or unreliable.	■ Bad adapter in a device. Check hardware. ■ Full-duplex or half-duplex Ethernet settings incorrect. ■ Cabling problem. Check connected LED. Check for correct cable properly attached and if length exceeds maximum cable distance.
Attached terminal or modem connection cannot communicate with router or switch.	■ Misconfigured terminal and console port. Check that baud rate and character format match. ■ Check if a default route is needed on router to reach switch on a different IP subnet.
Local VLAN devices cannot communicate with remote devices on a VLAN beyond the router.	■ Misconfigured IP addressing or mask. Check with CDP and show interface commands. ■ Default gateway not specified or incorrect. Check router, switch, servers, and clients. ■ VLAN misconfigured. Check port assignments. Eliminate unnecessary connections between VLANs if a port belongs to multiple VLANs. ■ VLAN inconsistency problem. Make sure VLANs match on both sides of a trunk. ■ ISL problem. Make sure there is proper trunking, use VLAN 1, and make sure that no valid VTP server information update has occurred.

When faced with poor throughput problems, check to see what type of errors exist. There could be a bad adapter card. Combinations of frame check sequence (FCS) and alignment errors and runs generally point to a duplex mismatch; the usual culprit is the autonegotiation between devices or a mismatched setting between the two sides of a link. Consider these questions:

- Is the problem on the local side or remote side of the link? Remember, a minimum number of switch ports is involved in a link.
- What path is the packet taking? Is it going across trunks or nontrunks to other switches?

If you see that the number of collisions in output from a **show interface** command is increasing rapidly, the problem may just be an overloaded link.

There is a myth that switched Ethernet eliminates collisions. The fact is that switches minimize the number of collisions, but if running in half-duplex mode, the collisions will still occur because two devices can always attempt to communicate at the same time.

An example is a news server that has many clients attempting to communicate at the same time. The traffic comes through the router and switch to the directly connected server. At the same time, the server is attempting to communicate back to these clients.

As the server is answering one client, another client sends a request; as a result, there is the potential for collision. The only cure for collisions on Ethernet is to run in full-duplex mode.

Problem: One Device Cannot Communicate with Another

Cisco.com

- **Make sure the IP address, subnet mask, and VLAN membership of the switch interface is correct.**
- **If the host is in the same subnet as the switch interface, make sure the switch interface and the switch port to which the host is connected are assigned to the same VLAN.**
- **If the host is in a different subnet, make sure the default gateway on the switch is configured with the address of a router in the same subnet as the switch interface.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-23

Problem: One device cannot communicate with another device.

The following are suggested solutions to the problem:

- Make sure that the IP address, subnet mask, and VLAN membership of the switch interface is correct by using the **show interface** command. To prevent conflicts, make sure the interfaces are configured with IP addresses and subnet masks in different subnets.
- If the host is in the same subnet as the switch interface, make sure that the switch interface and the switch port to which the host is connected are assigned to the same VLAN. Use the **show interface** and **show port** commands.
- If the host is in a different subnet, make sure that the default gateway (default route) on the switch is configured with the address of a router in the same subnet as the switch interface. Use the **show ip route** command.

Problem: One Device Cannot Communicate with Another (Cont.)

Cisco.com

- If the port is in listening or learning mode, wait until the port is in forwarding mode and try to connect to the host again.
- Make sure the speed and duplex settings on the host and the appropriate switch ports are correct.
- If the connected device is an end station, enable spanning-tree PortFast, disable trunking, and disable channeling on the port.
- Make sure the switch is learning the MAC address of the host.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-24

- Check the spanning-tree state on the port using the **show spantree** (Catalyst 1900 series) or **show spanning-tree vlan** (Catalyst 2950 series) command. If the port is in listening or learning mode, wait until the port is in forwarding mode and try to connect to the host again.
- Make sure that the speed and duplex settings on the host and the appropriate switch ports are correct. Use the **show port** command.
- If the connected device is an end station:
 - Enable spanning-tree PortFast on the port. Use the **set spantree portfast enable** command. PortFast places the port in forwarding mode immediately, bypassing listening and learning modes (do not use this feature for connections to non-end station devices).
 - Disable trunking on the port. Use the **set trunk** command.
 - Disable channeling on the port. Use the **set port channel** command. You must specify a valid port range with this command. You cannot specify a single port.
- Make sure that the switch is learning the MAC address of the host. Use the **show cam dynamic** command.

Problem: A Device Cannot Establish a Connection Across a Trunk Link

Cisco.com

- **Make sure the trunking mode configured on both ends of the link is valid. The trunking mode should be on or desirable on one end and on, desirable, or auto on the other end.**
- **Make sure the trunk encapsulation type configured on both ends of the link is valid.**
- **On IEEE 802.1Q trunks, make sure the native VLAN is the same on both ends of the trunk.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-25

Problem: A device cannot establish a connection across a trunk link.

The following are suggested solutions to the problem:

- Make sure that the trunking mode configured on both ends of the link is valid. The trunking mode should be on or desirable on one end and on, desirable, or auto on the other end. Use the **show trunk** (Catalyst 1900 series) or **show interface** (Catalyst 2950 series) command.
- Make sure that the trunk encapsulation type configured on both ends of the link is valid. Use the **show trunk** (Catalyst 1900 series) or **show interface** (Catalyst 2950 series) command.
- On IEEE 802.1Q trunks, make sure that the native VLAN is the same on both ends of the trunk. Use the **show trunk** (Catalyst 1900 series) or **show interface** (Catalyst 2950 series) command.

Problem: VTP Not Updating Configuration on Other Switches

Cisco.com

- **Make sure the switches are connected through trunk links. VTP updates are exchanged only over trunk links.**
- **Make sure the VTP domain name is the same on the appropriate switches. VTP updates are exchanged only between switches in the same VTP domain.**
- **Check if the switch is in VTP transparent mode. Only switches in VTP server or VTP client mode update their VLAN configuration based on VTP updates from other switches.**
- **If you are using VTP passwords, you must configure the same password on all switches in the VTP domain.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-26

Problem: VTP is not updating the configuration on other switches when the VLAN configuration changes.

The following are suggested solutions to the problem:

- Make sure that the switches are connected through trunk links. VTP updates are exchanged only over trunk links. Use the **show trunk** (Catalyst 1900 series) or **show interface** (Catalyst 2950 series) command.
- Make sure that the VTP domain name is the same on the appropriate switches. VTP updates are only exchanged between switches in the same VTP domain. Use the **show vtp domain** command.
- Check to see if the switch is in VTP transparent mode. Only switches in VTP server or VTP client mode update their VLAN configuration based on VTP updates from other switches. Use the **show vtp domain** command.
- If you are using VTP passwords, you must configure the same password on all switches in the VTP domain. To clear an existing VTP password, use the **set vtp passwd 0** command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Before you create VLANs, you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network.**
- **You will configure IEEE 802.1Q to carry traffic for multiple VLANs over a single link on a multivendor network.**
- **ISL operates in a point-to-point environment to carry traffic for multiple VLANs over a single link.**
- **Most Catalyst desktop switches support a maximum of 64 active VLANs. The Catalyst 1900 series supports 1,024 VLANs with the Enterprise Edition software. Depending on the model, the 2950 series can support up to 250 VLANs.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-27

Summary (Cont.)

Cisco.com

- **After creating a VLAN, you can statically assign a port or a number of ports to that VLAN. A port can belong to only one VLAN at a time.**
- **You can verify the VLAN configuration using the show commands.**
- **As network topologies, business requirements, and individual assignments change, VLAN requirements also change.**
- **Misconfiguration of a VLAN is one of the most common errors in switched networks.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—2-28

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Next Steps

After completing this lesson, go to:

- Lab Exercise 2-1: Configuring a Switch for Extended Functionality

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which Cisco IOS command enables VTP pruning on a Catalyst 1900 series switch?
- A) **vtp pruning**
 - B) **vtp pruning on**
 - C) **vtp pruning enable**
 - D) **vtp enable pruning**
- Q2) Which Cisco IOS command disables VTP pruning on a Catalyst 2950 series switch?
- A) **no vtp pruning**
 - B) **vtp pruning off**
 - C) **vtp pruning disable**
 - D) **vtp disable pruning**
- Q3) Which command correctly configures a switch in the VTP domain called “switchlab”?
- A) **vtp switchlab**
 - B) **vtp name switchlab**
 - C) **vtp domain switchlab**
 - D) **vtp domain name switchlab**
- Q4) When you configure 802.1Q trunks on Catalyst switches, which limitation is imposed?
- A) You must configure loops before disabling the STP.
 - B) You must configure the native VLAN uniquely on each end of the trunk link.
 - C) You must configure the native VLAN the same on both ends of the trunk link.
 - D) You must configure ISL on one end of the trunk link, and 802.1Q on the other end of the trunk link.
- Q5) Which Cisco IOS command correctly configures an 802.1Q trunk on a Catalyst 2950 series switch?
- A) **switchport mode trunk**
 - B) **switchport trunk mode**
 - C) **switchport trunk encapsulation isl**
 - D) **switchport trunk encapsulation dot1q**

- Q6) Which Cisco IOS command enables ISL trunking on a Catalyst 1900 series Fast Ethernet switch port?
- A) **trunk on**
 - B) **encapsulation isl**
 - C) **encapsulation trunk**
 - D) **encapsulation trunk isl**
- Q7) Match each **trunk** command option to its description.
- | | |
|----------|---------------------|
| _____ 1. | on |
| _____ 2. | off |
| _____ 3. | auto |
| _____ 4. | desirable |
| _____ 5. | nonnegotiate |
- A) triggers the port to negotiate the link from nontrunk to trunk mode
 - B) enables a port to become a trunk only if the connected device has the state set to on or desirable
 - C) disables port trunk mode and negotiates with the connected device to convert the link to nontrunk
 - D) configures the port to permanent ISL trunk mode and no negotiation takes place with the partner
 - E) configures the port into permanent ISL trunk mode and negotiates with the connected device to convert the link to trunk mode
- Q8) By default, a switch is in VTP _____ mode so that you can add, change, or delete VLANs. If the switch is set to VTP _____ mode, you cannot add, change, or delete VLANs.
- A) client, server
 - B) server, client
 - C) client, transparent
 - D) server, transparent
- Q9) Which Cisco IOS command do you use to change the name of a VLAN on a Catalyst switch?
- A) **vlan name *name***
 - B) **vlan *number* name *name***
 - C) **vlan oldname *name* newname *name***
 - D) **vlan number oldname *name* newname *name***

- Q10) What does the **vlan-membership** command do on the Catalyst 1900 series switch?
- A) configures VTP domain membership
 - B) assigns a port as a member of a VLAN
 - C) configures VMPS address to VLAN mappings
 - D) assigns the address of the VMPS server to be used for VLAN membership
- Q11) To how many VLANs can a nontrunk port of a Catalyst 1900 series or 2950 series switch belong?
- A) 1
 - B) 2
 - C) 64
 - D) up to the number of active VLANs on the switch
- Q12) Which Cisco IOS command displays the VTP configuration parameters on a Catalyst 2950 series switch?
- A) **show ip**
 - B) **show version**
 - C) **show vtp status**
 - D) **show vtp config**
- Q13) Which Cisco IOS command displays the VLAN assignment and membership type for a particular port on a Catalyst 1900 series switch?
- A) **show ip**
 - B) **show vlan**
 - C) **show version**
 - D) **show interfaces**
- Q14) What is the impact of using **no switchport access vlan** command on the Catalyst 2950 series switch while in the interface configuration mode?
- A) Port is removed from all VLANs.
 - B) Port is changed to trunking mode.
 - C) Port is configured as a secure port.
 - D) Port is reassigned to the default VLAN.
- Q15) Assuming default names have been assigned to VLANs, which Cisco IOS command should you use to remove the VLAN named VLAN0008?
- A) **no vlan 8**
 - B) **vlan 0008 delete**
 - C) **no vlan VLAN0008**
 - D) **no vlan name VLAN0008**

- Q16) Suppose the performance on a VLAN is slow or unreliable. Which three situations could cause the problem? (Choose three.)
- A) There is a cabling problem.
 - B) A device has a bad adapter.
 - C) The VLAN is misconfigured.
 - D) You may have an ISL problem.
 - E) The terminal and console port are not configured correctly.
 - F) The full-duplex or half-duplex Ethernet settings are incorrect.
- Q17) Switches minimize the collision domain, but if running in _____, the collisions will still occur because two devices can always attempt to communicate at the same time.
- A) full speed
 - B) full duplex
 - C) half duplex
 - D) a routed environment

Quiz Answer Key

- Q1) C
Relates to: Configuring VTP
- Q2) A
Relates to: Configuring VTP
- Q3) C
Relates to: Configuring VTP
- Q4) C
Relates to: Configuring 802.1Q Trunking
- Q5) A
Relates to: Configuring 802.1Q Trunking
- Q6) A
Relates to: Configuring ISL Trunking
- Q7) 1-D, 2-C, 3-B, 4-A, 5-E
Relates to: Configuring ISL Trunking
- Q8) B
Relates to: Configuring a VLAN
- Q9) B
Relates to: Configuring a VLAN
- Q10) B
Relates to: Assigning Ports to a VLAN
- Q11) A
Relates to: Assigning Ports to a VLAN
- Q12) C
Relates to: Verifying the VLAN Configuration
- Q13) B
Relates to: Verifying the VLAN Configuration
- Q14) D
Relates to: Executing Adds, Moves, and Changes for VLANs
- Q15) A
Relates to: Executing Adds, Moves, and Changes for VLANs
- Q16) A, B, F
Relates to: Troubleshooting VLANs
- Q17) C
Relates to: Troubleshooting VLANs

Lesson Assessments

Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

Outline

This section includes these assessments:

- Lesson Assessment 2-1: VLAN Operation Overview
- Lesson Assessment 2-2: Configuring VLANs

Lesson Assessment 2-1: VLAN Operation Overview

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of a VLAN, VLAN Trunking Protocol, IEEE 802.1Q trunking, and Inter-Switch Link trunking

Quiz

Answer these questions:

- Q1) Which three statements best describe VLANs? (Choose three.)
- A) A VLAN connects to bridges.
 - B) A VLAN can connect across WANs.
 - C) A VLAN can exist on a single switch.
 - D) A VLAN cannot exist on multiple switches.
 - E) A VLAN shares broadcasts on different VLANs.
 - F) A VLAN can include multiple-building infrastructures.
- Q2) A VLAN permits a group of users to share a common _____ regardless of their physical location in the network.
- A) LAN segment
 - B) collision domain
 - C) broadcast domain
 - D) Internet connection
- Q3) What feature is required for a VLAN to span two switches?
- A) a trunk to connect the switches
 - B) a router to connect the switches
 - C) a bridge to connect the switches
 - D) a VLAN configured between the switches
- Q4) Where does the Catalyst switch transmit a frame that arrives on a switch port?
- A) to the uplink port on the switch
 - B) only to ports that belong to the same VLAN
 - C) to ports on all VLANs configured on the switch
 - D) only to ports on the same physical LAN segment
- Q5) A VLAN Membership Policy Server (VMPS) contains a database that maps _____ to VLAN assignment.
- A) host IDs
 - B) usernames
 - C) IP addresses
 - D) MAC addresses

- Q6) Match each VLAN membership mode to its description.
- _____ 1. static
- _____ 2. dynamic
- A) An administrator configures the VLAN port.
- B) When a frame arrives on a port, the switch queries a VMPS for its LAN assignment based on the source MAC address of the frame.
- Q7) What does PVST+ allow on a switched network?
- A) allows printers to share network resources
- B) runs a single STP instance over an ISL network
- C) allows creation of a multiple spanning-tree network
- D) allows running several STP instances, even over an 802.1Q network
- Q8) What type of network structure does a PVST+ network require?
- A) star structure
- B) ring structure
- C) tree-like structure
- D) hierarchical structure
- Q9) For which two reasons do network administrators use ISL? (Choose two.)
- A) to maintain redundant links
- B) to allow clients to see the ISL header
- C) to provide interVLAN communications over a bridge
- D) to provide trunking between Cisco switches and other vendor switches
- E) to load-balance traffic between parallel links using the Spanning Tree Protocol
- Q10) To support the ISL feature, each connecting device must be _____.
- A) ISL-capable
- B) running Cisco IOS
- C) VLAN-capable
- D) 802.1Q-capable
- Q11) What primary benefit does VTP offer?
- A) allows trunking to provide redundancy
- B) minimizes redundancy on a switched network
- C) allows you to run several VLANs over a single trunk
- D) minimizes misconfigurations and configuration inconsistencies
- Q12) How many VTP domains can you configure for a switch?
- A) 1
- B) 2
- C) 4
- D) 8

- Q13) How often are VTP advertisements sent on a VLAN when there is no change?
- A) every 2 seconds
 - B) every 30 seconds
 - C) every 90 seconds
 - D) every 300 seconds
- Q14) Which two statements describe VTP pruning? (Choose two.)
- A) VTP pruning increases available bandwidth.
 - B) VTP pruning decreases available bandwidth.
 - C) VTP pruning requires that static VLAN information be configured on a trunk port.
 - D) VTP pruning uses VLAN advertisements to determine when VLAN traffic is on a trunk needlessly.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 2-2: Configuring VLANs

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Use Cisco IOS commands to configure VLANs, VTP, IEEE 802.1Q trunking, and Inter-Switch Link trunking, given a functioning access layer switch
- Execute an add, move, or change on an access layer switch, given a new network requirement
- Use **show** commands to identify anomalies in VLAN, VTP, IEEE 802.1Q trunking, Inter-Switch Link trunking, and spanning-tree operation within a VLAN, given an operational access layer switch
- Use **debug** commands to identify events and anomalies in VLAN, VTP, IEEE 802.1Q trunking, Inter-Switch Link trunking, and spanning-tree operation, given an operational access layer switch

Quiz

Answer these questions:

- Q1) Which command correctly configures a switch for transparent mode in the VTP domain called “switchlab”?
- A) **vtp trunk on**
 - B) **vtp transparent**
 - C) **vtp domain switchlab**
 - D) **vtp domain switchlab transparent**
- Q2) What is the default VTP mode on a Catalyst switch?
- A) off
 - B) client
 - C) server
 - D) transparent
- Q3) If you group 802.1Q trunks into EtherChannel port groups, what guideline must you follow?
- A) Each port in the group must be a secure port.
 - B) Each trunk in the group can have its own configuration.
 - C) All ports must follow the parameters set for the first port to be added to the group.
 - D) All trunks must follow the parameters set for the first trunk to be added to the group.

- Q4) Which Cisco IOS command correctly configures ISL encapsulation for an ISL trunk on a Catalyst 1900 series switch?
- A) **trunk on**
 - B) **switchport mode trunk**
 - C) **trunk encapsulation isl**
 - D) **switchport trunk encapsulation isl**
- Q5) Which feature manages automatic trunk negotiation?
- A) IEEE 802.1Q
 - B) port grouping
 - C) Dynamic Trunk Protocol (DTP)
 - D) VLAN Trunking Protocol (VTP)
- Q6) When you use the **nonnegotiate** option with the **trunk** interface configuration command, how is the trunk configured?
- A) configures the port to permanent ISL or 802.1Q trunk mode
 - B) triggers the port to negotiate the link from nontrunk to trunk mode
 - C) disables port trunk mode and negotiates the connected device to convert the link to nontrunk
 - D) enables a port to become a trunk only if the connected device has the state set to on or desirable
- Q7) What is the logical sequence for configuring a Catalyst switch port to be in VLAN 3?
- A) Create the VLAN, and then assign the port to the VLAN.
 - B) Assign the port to the VLAN; all VLANs are created by default.
 - C) Create the VLAN, assign ports to the VLAN, then configure VTP.
 - D) Assign the port to the VLAN; this also creates the VLAN with a default name.
- Q8) Which command modifies an existing VLAN name?
- A) **vlan database**
 - B) **change trunk desirable**
 - C) **vlan vlan# name vlan_name**
 - D) **change vlan *vlan#* name *vlan_name***
- Q9) Assigning switch ports to VLANs using the manual method is known as port-based, or _____, VLAN membership.
- A) static
 - B) manual
 - C) dynamic
 - D) individual
- Q10) After creating a VLAN, you can statically assign a port or a number of ports to that VLAN. A port can belong to _____ at a time.
- A) only one VLAN
 - B) up to 64 VLANs
 - C) up to 128 VLANs
 - D) one or two VLANs

- Q11) The **show vlan-membership** command is used on a Catalyst 1900 series switch to _____.
- A) display the VTP domain parameters
 - B) display the VMPS server configuration parameters
 - C) display which ports are members of which VLANs
 - D) display the names of the VLANs and the ports assigned to the VLANs
- Q12) Which command displays the spanning-tree configuration status of the ports on a Catalyst 2950 series switch?
- A) **show vlan**
 - B) **show trunk**
 - C) **show spanning-tree**
 - D) **show spantree config**
- Q13) When you are deleting a VLAN from a VTP domain, where should the change be performed?
- A) on a switch in VTP server mode
 - B) on every switch in VTP client mode
 - C) on a switch in VTP transparent mode
 - D) on every switch, regardless of VTP mode
- Q14) What precaution should you take when redeploying a switch to a new VTP domain in the network?
- A) Set a unique VTP password on the switch for security.
 - B) Preconfigure all VLANs in new VTP domain on the switch.
 - C) Verify that VTP revision number is lower than existing domain.
 - D) Configure the switch to VTP transparent mode to minimize impact.
- Q15) If a device on a VLAN cannot establish a connection across a trunk link, which three actions should you take to resolve the problem? (Choose three.)
- A) Make sure the trunking mode configured on both ends of the link is valid.
 - B) Make sure the trunk encapsulation type configured on both ends of the link is valid.
 - C) Make sure the port is connected and is not receiving any physical-layer (alignment or FCS) errors.
 - D) Make sure the port is trunking and that the allowed VLAN list allows the desired VLAN range to pass through.
 - E) If the host is on the same subnet as the switch interface, make sure the switch interface and switch port to which the host is connected are assigned to the same VLAN.

- Q16) Suppose that VTP is not updating the configuration on other switches when the VLAN configuration changes. What command would you use to determine if the switch is in VTP transparent mode?
- A) **show trunk**
 - B) **show spantree**
 - C) **show interfaces**
 - D) **show vtp domain**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment Answer Key

Lesson Assessment 2-1: VLAN Operation Overview

- Q1) B, C, F
- Q2) C
- Q3) A
- Q4) B
- Q5) D
- Q6) A, B
- Q7) D
- Q8) C
- Q9) A, E
- Q10) A
- Q11) D
- Q12) A
- Q13) D
- Q14) A, D

Lesson Assessment 2-2: Configuring VLANs

- Q1) B
- Q2) C
- Q3) C
- Q4) A
- Q5) C
- Q6) A
- Q7) A
- Q8) C
- Q9) A
- Q10) A
- Q11) C
- Q12) C
- Q13) A
- Q14) C
- Q15) A, B, D
- Q16) D

Determining IP Routes

Overview

Routing is the process of determining where to send data packets that are destined for addresses outside the local network. Routers gather and maintain routing information to enable the transmission and receipt of such data packets. Conceptually, routing information takes the form of entries in a routing table, with one entry for each identified route. The network administrator can statically (manually) configure entries in the routing table or the router can create and maintain the routing table dynamically to accommodate network changes whenever they occur. This module describes the features and operation of Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF) routing protocols, and shows you how to configure and troubleshoot each.

Upon completing this module, you will be able to:

- Describe the features and operation of static routing
- Describe the features and operation of dynamic routing protocols, including RIP, IGRP, EIGRP, and OSPF
- Build a functional router configuration to support the specified network operational requirements, given a network design
- Use **show** commands to identify anomalies in routing operation, given an operational router
- Use **debug** commands to identify events and anomalies in routing operation, given an operational router

Outline

The module contains these lessons:

- Routing Overview
- Distance Vector Routing
- Link-State and Balanced Hybrid Routing
- Enabling RIP
- Enabling IGRP
- Enabling EIGRP
- Enabling OSPF
- Variable-Length Subnet Masks
- Lesson Assessments

Routing Overview

Overview

Routing is the process of determining where to send data packets destined for addresses outside the local network. Routers gather and maintain routing information to enable the transmission and receipt of such data packets. Conceptually, routing information takes the form of entries in a routing table, with one entry for each identified route. The network administrator can statically (manually) configure the entries in the routing table or the router can use a routing protocol to create and maintain the routing table dynamically to accommodate network changes whenever they occur. This lesson introduces IP static and dynamic routing.

Relevance

To effectively manage an IP network, you must understand how the different types of routing protocols operate and understand the benefits and limitations with each routing protocol.

Objectives

Upon completing this lesson, you will be able to:

- Explain the differences between static routing and dynamic routing
- Identify the classes of routing protocols
- Use Cisco IOS commands to configure static routes and default route forwarding, given a functioning router
- Use **show** commands to identify anomalies in static routing operation, given an operational router
- Describe the operation of “router on a stick”
- Configure router on a stick for interVLAN routing using Inter-Switch Link or 802.1Q trunking, given an operational switch and router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

Outline

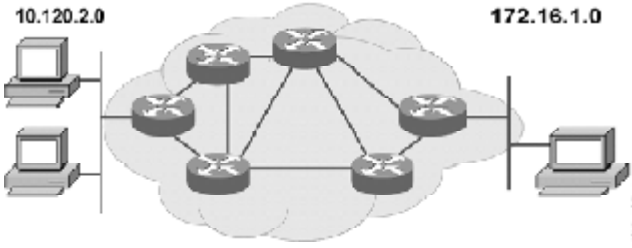
The lesson includes these topics:

- Overview
- Introducing Routing
- Comparing Static and Dynamic Routes
- Configuring Static Routes
- Configuring Default Route Forwarding
- Verifying the Static Routing Configuration
- Introducing Dynamic Routing Protocols
- Using the **ip classless** Command
- InterVLAN Routing
- Summary
- Quiz

Introducing Routing

Routing is the process by which an item gets from one location to another. Many items get routed: for example, mail, telephone calls, and trains. In networking, a router is the device used to route traffic. This topic introduces the basic operation of a router or other entity that performs routing.

What Is Routing?



To route, a router needs to do the following:

- **Know the destination address**
- **Identify the sources it can learn from**
- **Discover possible routes**
- **Select the best route**
- **Maintain and verify routing information**

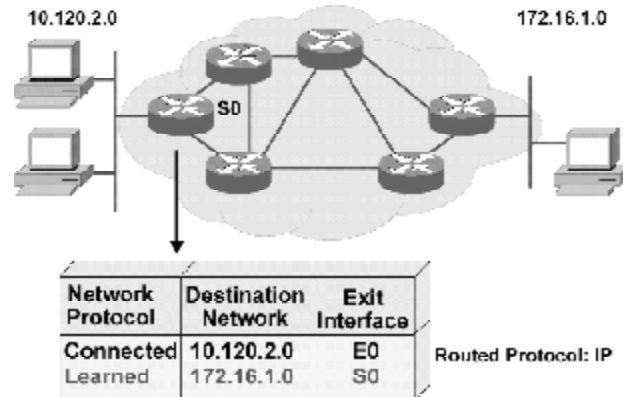
© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-6

To be able to route anything, a router, or any other entity that performs the routing, must do the following:

- **Know the destination address:** What is the destination (or address) of the item that needs to be routed?
- **Identify sources of routing information:** From which source (other routers) can the router learn the paths to given destinations?
- **Discover routes:** What are the initial possible routes, or paths, to the intended destinations?
- **Select routes:** What is the best path to the intended destination?
- **Maintain and verify routing information:** Are the known paths to destinations the most current?

What Is Routing? (Cont.)

Cisco.com



- **Routers must learn destinations that are not directly connected.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3.7

The routing information that a router obtains from other routers is placed in its routing table. The router will rely on this table to tell it which interfaces to use when forwarding addressed packets.

If the destination network is directly connected, the router already knows the interface to use when forwarding packets.

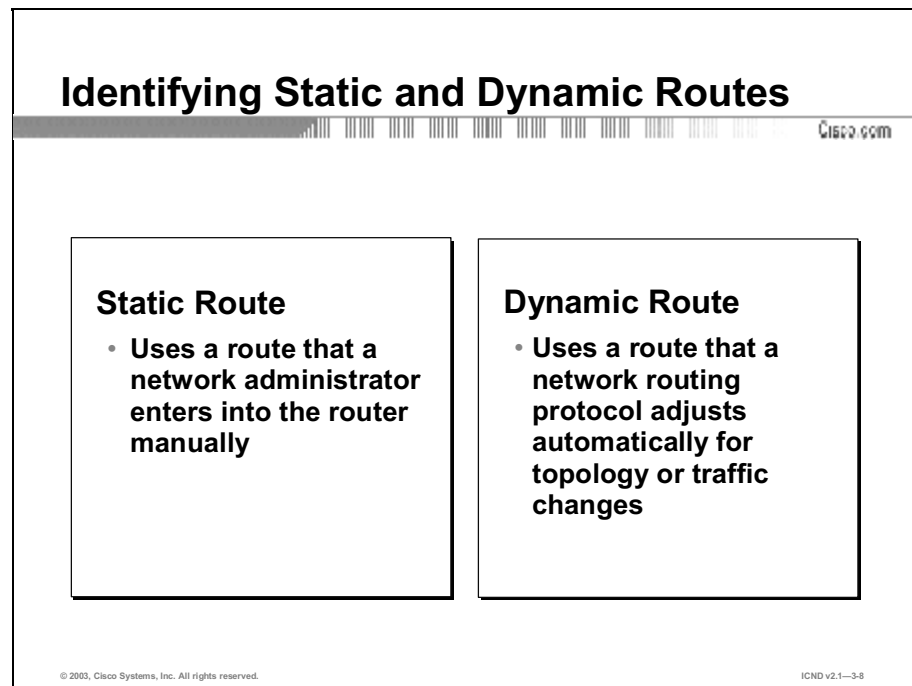
If destination networks are not directly attached, then the router must learn the best route to use when forwarding packets.

This information can be learned in the following ways:

- Entered manually by the network administrator
- Collected through the dynamic routing process running in the routers

Comparing Static and Dynamic Routes

Routers can forward packets over static routes or dynamic routes, based on the router configuration. This topic explains the differences between static and dynamic routing.

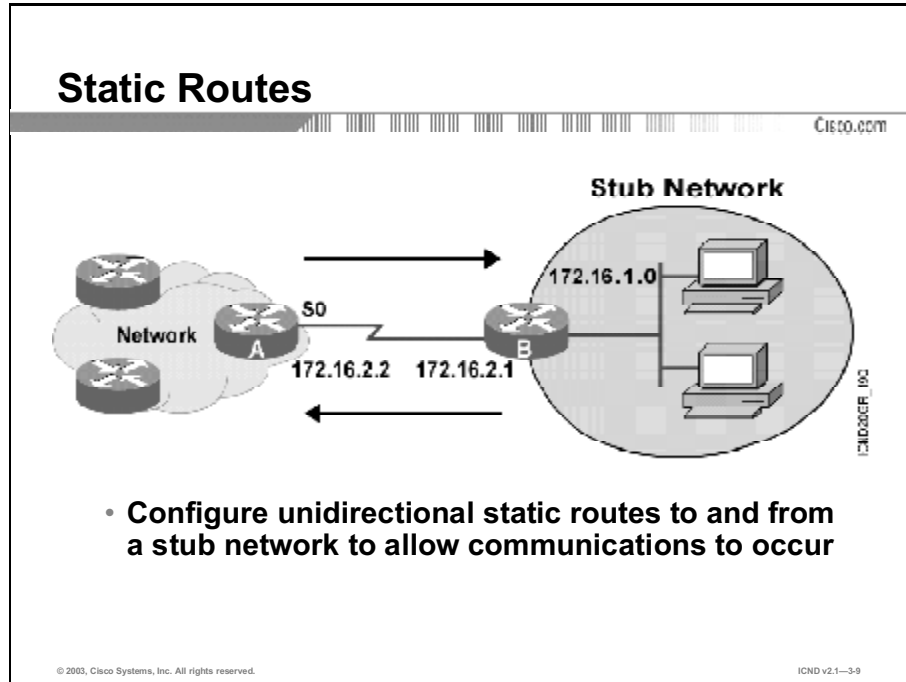


Two ways to tell the router where to forward the packets that are not directly connected are as follows:

- **Static routes:** The router learns routes when an administrator manually configures the static route. The administrator must manually update this static route entry whenever an internetwork topology change requires an update. Static routes are user-defined routes that specify the path that packets moving between a source and a destination take. These administrator-defined routes allow very precise control over the routing behavior of the IP internetwork.
- **Dynamic routes:** The router dynamically learns routes *after* an administrator configures a routing protocol that helps determine routes. Unlike the situation with static routes, after the network administrator enables dynamic routing, the routing process automatically updates route knowledge whenever new topology information is received. The router learns and maintains routes to the remote destinations by exchanging routing updates with other routers in the internetwork.

Configuring Static Routes

Static routes may be useful for stub networks and for specifying a “gateway of last resort” to which all packets with an unknown destination address will be sent. This topic shows you how to configure static routes on Cisco routers.



Static routes are commonly used when routing from a network to a stub network. A stub network (sometimes called a leaf node) is a network accessed by a single route. Often, static routes are used to reach a stub network.

In the figure, router A will be configured with a static route to reach the 172.16.1.0 subnet via its serial interface. Router B will be configured with a static or default route to reach the networks behind router A via its serial interface.

Note	The static route is configured for connectivity to remote networks that are not directly connected to your router. For end-to-end connectivity, a static route must be configured in both directions.

Static Route Configuration

Cisco.com

```
Router(config)#ip route network [mask]  
{address | interface} [distance] [permanent]
```

- Defines a path to an IP destination network or subnet or host

© 2003, Cisco Systems, Inc. All rights reserved.

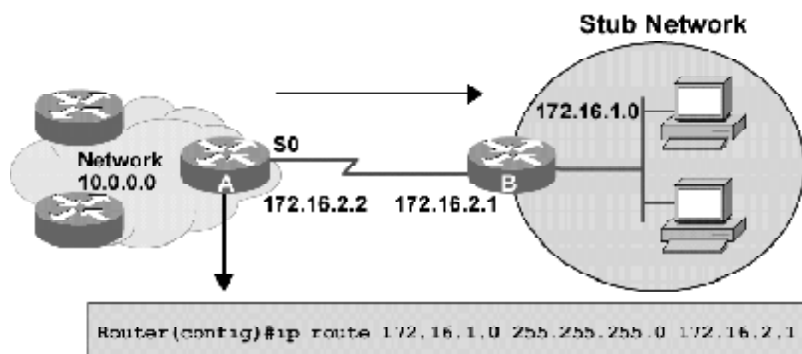
ICND v2.1—3-10

To configure a static route, enter the **ip route** command in global configuration mode. The following parameters further define the static route. A static route allows manual configuration of the routing table. No dynamic changes to this table entry will occur as long as the path is active.

ip route Command Parameters	Description
<i>network</i>	Destination network or subnet or host.
<i>mask</i>	Subnet mask.
<i>address</i>	IP address of next-hop router.
<i>interface</i>	Name of the interface to use to get to destination network. The interface should be a point-to-point interface. The command will not work properly if the interface is multiaccess (for example, a shared media Ethernet interface).
<i>distance</i>	(Optional) Defines the administrative distance. Administrative distance is covered later in this lesson.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.

Static Route Example

Cisco.com



- This is a unidirectional route. You must have a route configured in the opposite direction.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-11

In the example, the static route is configured as follows:

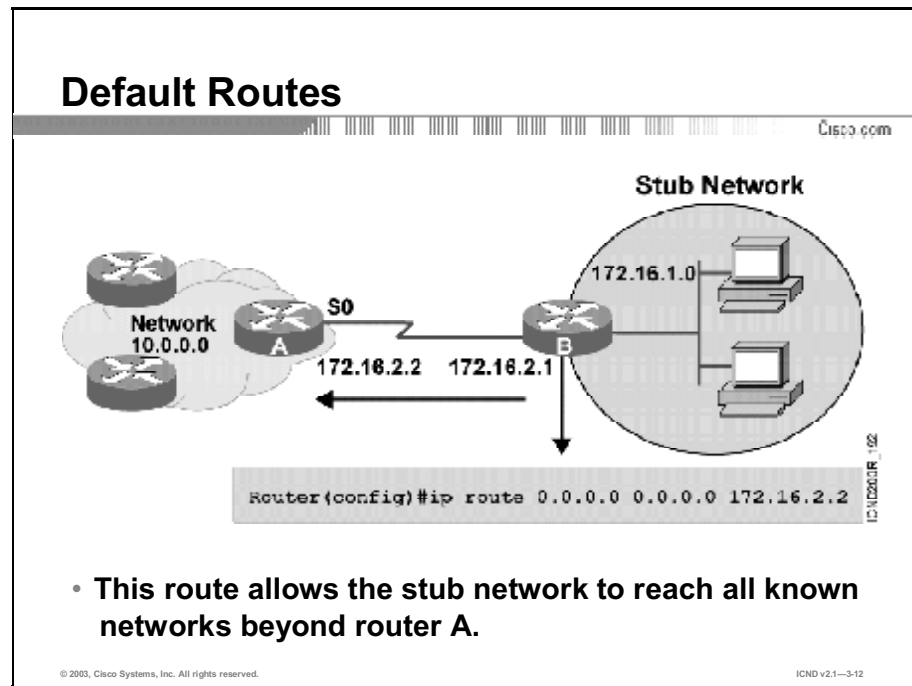
```
Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

ip route Command Parameters	Description
ip route	Identifies the static route command.
172.16.1.0	Specifies a static route to the destination subnetwork.
255.255.255.0	Indicates the subnet mask. (8 bits of subnetting are in effect.)
172.16.2.1	IP address of next-hop router in the path to the destination.

The assignment of a static route to reach the stub network 172.16.1.0 is proper for router A because there is only one way to reach that network.

Configuring Default Route Forwarding

A default route is a special type of static route. A default route is a route to use in situations when the route from a source to a destination is not known or when it is unfeasible for the router to maintain many routes in its routing table. This topic explains how to configure default route forwarding.



You will use the **ip route** command to configure default route forwarding. In the figure, router B is configured to forward all packets for which the destination network is not explicitly listed in its routing table to router A.

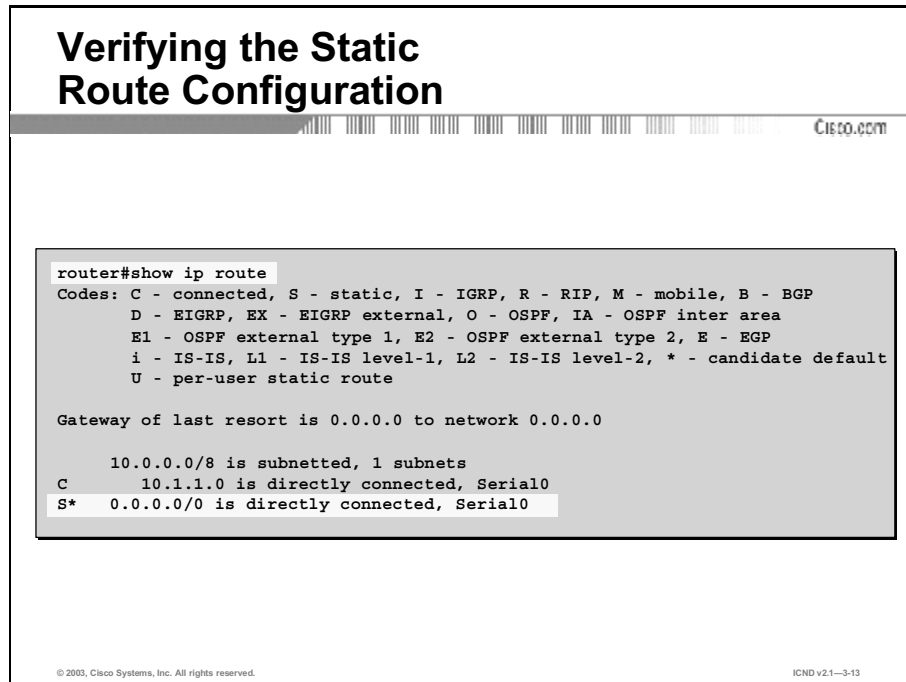
In the default route example, the following applies:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

ip route Command Parameters	Description
ip route	Identifies the static route command.
0.0.0.0	Routes to nonexistent subnet. (With a special mask, it denotes the default network.)
0.0.0.0	Special mask indicating the default route.
172.16.2.2	IP address of the next-hop router to be used as the default for packet forwarding.

Verifying the Static Routing Configuration

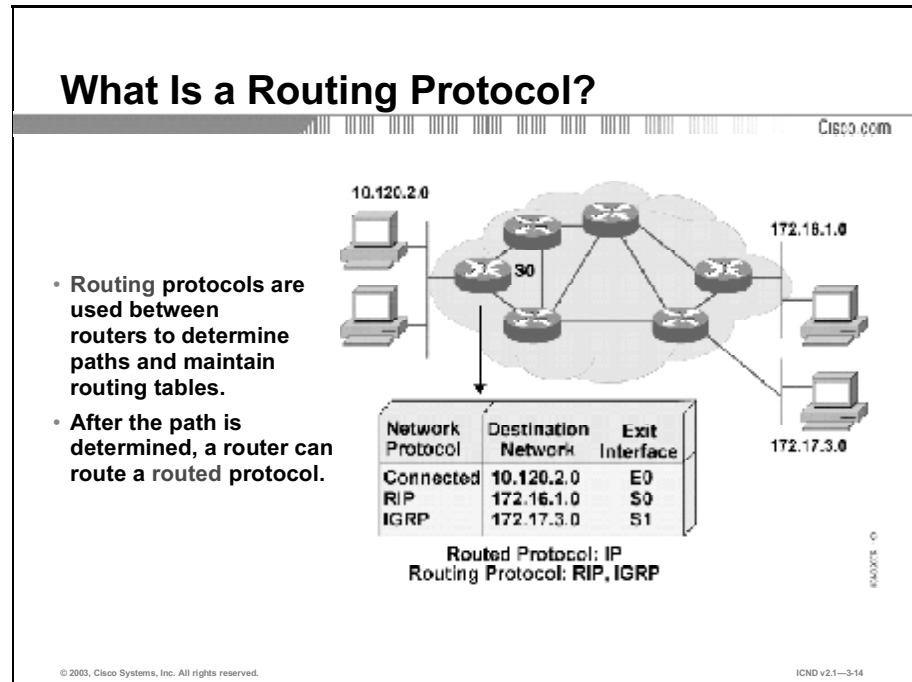
When the static routing configuration is complete, use the **show ip route** command to verify the configuration. This topic provides an example showing you how to verify the static routing configuration.



To verify that you have properly configured static routing, enter the **show ip route** command and look for static routes signified by the “S.” You should see a verification output like the example shown in the figure. The asterisk (*) indicates the last path used when a packet was forwarded.

Introducing Dynamic Routing Protocols

Dynamic routing relies on a routing protocol to disseminate knowledge. A routing protocol defines the rules that are used by a router when it communicates with neighboring routers. This topic introduces the features offered by dynamic routing protocols.



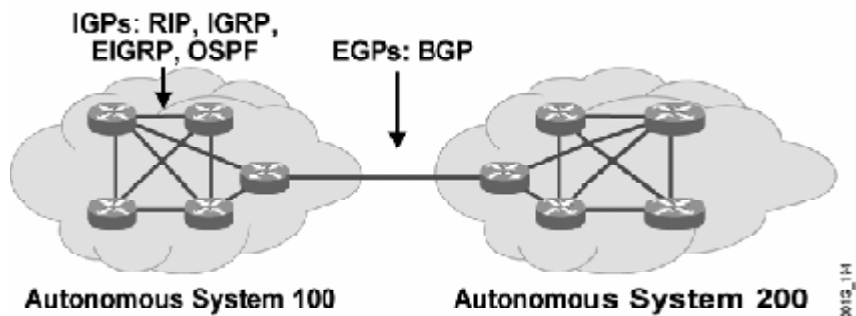
A routing protocol is a network layer protocol that interprets information in a network layer address to allow a packet to be forwarded to the destination network. (In contrast, routed protocols define the format and use of the fields within a packet. Packets generally are conveyed from end system to end system.)

Further examples of the types of information that routing protocols describe are as follows:

- Routing protocols describe how updates are conveyed.
- Routing protocols describe what knowledge is conveyed.
- Routing protocols describe when to convey knowledge.
- Routing protocols describe how to locate recipients of the updates.

Autonomous Systems: Interior or Exterior Routing Protocols

Cisco.com



- An autonomous system is a collection of networks under a common administrative domain.
- IGPs operate within an autonomous system.
- EGPs connect different autonomous systems.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-15

Two major types of routing protocols are as follows:

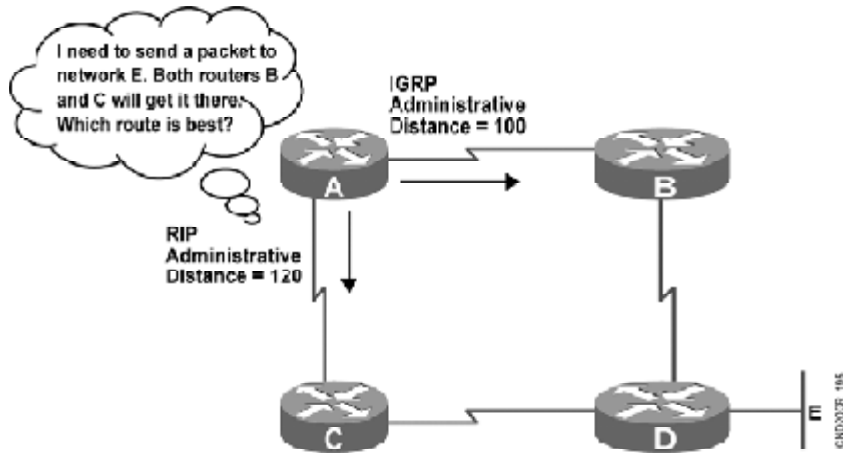
- **Interior Gateway Protocols (IGPs):** Routing protocols used to exchange routing information within an autonomous system. Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF) are examples of IGPs.
- **Exterior Gateway Protocols (EGPs):** Used to connect between autonomous systems. An autonomous system is a collection of networks under a common administration and sharing a common routing strategy. Border Gateway Protocol (BGP) is an example of an EGP.

The Internet Assigned Numbers Authority (IANA) is the umbrella responsible for allocating autonomous system numbers. Specifically, the American Registry for Internet Numbers (ARIN) has the jurisdiction for assigning numbers for the Americas, Caribbean, and Africa. Réseaux IP Européennes-Network Information Center (RIPE-NIC) administers the numbers for Europe, and the Asia Pacific Network Information Center (APNIC) administers the autonomous system numbers for the Asia-Pacific region. This autonomous system designator is a 16-bit number.

Note Use of the IANA-assigned autonomous system number rather than some other number is needed only if your organization plans to use an EGP such as BGP.

Administrative Distance: Ranking Routes

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-16

Multiple routing protocols and static routes may be used at the same time. If there are several sources for routing information, an administrative distance value is used to rate the trustworthiness of each routing information source. By specifying administrative distance values, Cisco IOS software can discriminate between sources of routing information. For each destination learned, Cisco IOS software always places the route from the source with the lowest administrative distance in the routing table.

An administrative distance is an integer from 0 to 255. A routing protocol with a lower administrative distance is more trustworthy than one with a higher administrative distance. As shown in the figure, if router A receives a route to network E from IGRP and RIP at the same time, and because RIP and IGRP use incompatible routing metrics, router A would use the administrative distance to determine that IGRP is more believable, and would add the IGRP route to the routing table. The table shows the default administrative distance for selected routing information sources.

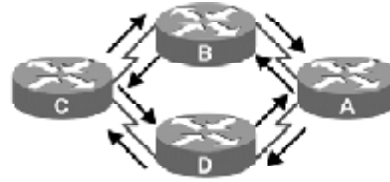
Route Source	Default Distance
Connected interface	0
Static route address	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown/unbelievable	255 (will not be used to pass traffic)

If nondefault values are necessary, a network administrator can use Cisco IOS software to configure administrative distance values on a per-router, per-protocol, and per-route basis.

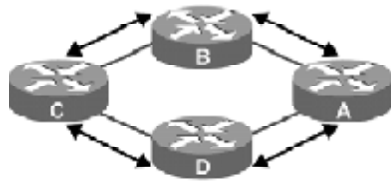
Classes of Routing Protocols

Cisco.com

Distance Vector



Hybrid Routing



Link State

ICND2004_118

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-17

Within an autonomous system, most IGP routing algorithms can be classified as conforming to one of the following algorithms:

- **Distance vector:** The distance vector routing approach determines the direction (vector) and distance (hops) to any link in the internetwork.
- **Link state:** The link state, also called shortest path first, approach creates an abstraction of the exact topology of the entire internetwork, or at least the partition in which the router is situated.
- **Balanced hybrid:** A balanced hybrid approach combines aspects of the link state and distance vector algorithms.

There is no single best routing algorithm for all internetworks. All routing protocols provide the information differently.

Classful Routing Overview

Cisco.com

- **Classful routing protocols do not include the subnet mask with the route advertisement.**
- **Within the same network, consistency of the subnet masks is assumed.**
- **Summary routes are exchanged between foreign networks.**
- **Examples of classful routing protocols:**
 - **RIP Version 1 (RIPv1)**
 - **IGRP**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-18

Classful routing is a consequence of the fact that subnet masks are *not* advertised in the routing advertisements generated by most distance vector routing protocols.

When using a classful routing protocol, all subnets of the same major (class A, B, or C) network must use the same subnet mask. Routers running a classful routing protocol perform automatic route summarization across network boundaries.

Upon receiving a routing update packet, a router running a classful routing protocol does one of the following to determine the network portion of the route:

- If the routing update information contains the same major network number as configured on the receiving interface, the router applies the subnet mask that is configured on the receiving interface.
- If the routing update information contains a different major network as configured on the receiving interface, the router will apply the default classful mask (by address class):
 - For class A addresses, the default classful mask is 255.0.0.0.
 - For class B addresses, the default classful mask is 255.255.0.0.
 - For class C addresses, the default classful mask is 255.255.255.0.

Classless Routing Overview

Cisco.com

- **Classless routing protocols include the subnet mask with the route advertisement.**
- **Classless routing protocols support variable-length subnet mask (VLSM).**
- **Summary routes can be manually controlled within the network.**
- **Examples of classless routing protocols:**
 - **RIP Version 2 (RIPv2)**
 - **EIGRP**
 - **OSPF**
 - **IS-IS**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-19

Classless routing protocols can be considered second-generation protocols because they are designed to address some of the limitations of the earlier classful routing protocols. One of the most serious limitations in a classful network environment is that the subnet mask is not exchanged during the routing update process, thus requiring the same subnet mask to be used on all subnetworks within the same major network.

Another limitation of the classful approach is the need to automatically summarize to the classful network boundary at major network boundaries.

In the classless environment, the summarization process is controlled manually and can usually be invoked at any bit position within the address. Because subnet routes are propagated throughout the routing domain, manual summarization may be required to keep the size of the routing tables manageable.

Routing Protocol Comparison Chart

Cisco.com

Characteristic	RIPv1	IGRP	EIGRP [*]	IS-IS	OSPF
Distance vector	X	X	X		
Link state				X	X
Automatic route summarization	X	X	X		
Manual route summarization			X	X	X
VLSM support			X	X	X
Proprietary		X	X		
Convergence time	Slow	Slow	Very Fast	Fast	Fast

^{*}EIGRP is an advanced distance vector protocol with some link features.

© 2003, Cisco Systems, Inc. All rights reserved.

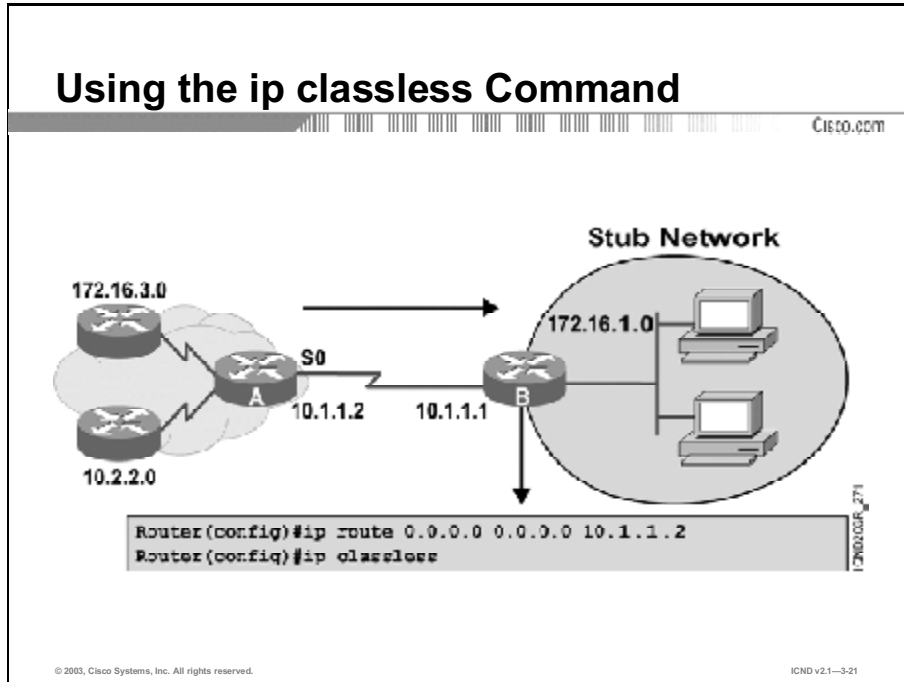
ICND v2.1—3-20

The figure compares some of the characteristics of the different routing protocols.

EIGRP generally has the fastest convergence time because it maintains a feasible successor (backup route) in its topology table. Therefore, if the best path goes down, it immediately switches to the feasible successor without a need to perform further best-path calculation.

Using the ip classless Command

The **ip classless** command prevents a router from dropping a packet destined for an unknown subnet of a directly attached network if a default route is configured. This topic describes how to use the **ip classless** command.



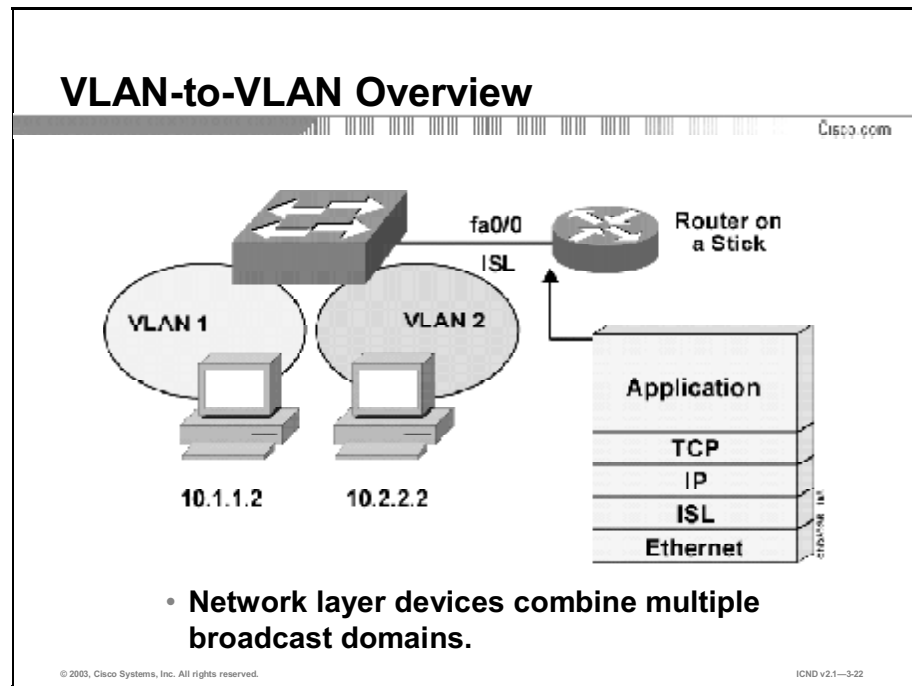
A classful router by default assumes that all subnets of a directly attached network will be present in the IP routing table. If a packet is received with a destination address within an unknown subnet of a directly attached network, the router assumes that the subnet does not exist and drops the packet. This behavior holds true even if the IP routing table contains a default route.

However, the administrator can change this behavior with the **ip classless** global configuration command (**ip classless** is enabled by default).

With **ip classless** configured, if a packet is received with a destination address within an unknown subnet of a directly attached network, the router will match it to the default route and forward it to the next hop that is specified by the default route.

InterVLAN Routing

In a VLAN environment, frames are switched only between ports within the same broadcast domain. Therefore, a Layer 3 device is required to enable *interVLAN* communication. Use Inter-Switch Link (ISL) or 802.1Q to enable trunking on a router subinterface. This topic describes interVLAN routing.



In a VLAN environment, frames are switched only between ports within the same “broadcast domain.” VLANs perform network partitioning and traffic separation at Layer 2. InterVLAN communication cannot occur without a Layer 3 device, such as a router.

The figure illustrates a router attached to a core switch. This configuration is sometimes referred to as a “router on a stick.” The router can receive packets on one VLAN and forward them to another VLAN. To perform interVLAN routing functions, the router must know how to reach all VLANs being interconnected. There must be a separate physical connection on the router for each VLAN and you must enable ISL or 802.1Q trunking on a single physical connection. The router already knows about directly connected networks. It must learn routes to networks not connected directly to it.

Dividing a Physical Interface into Subinterfaces

Cisco.com



- **Physical interfaces can be divided into multiple subinterfaces.**

© 2003, Cisco Systems, Inc. All rights reserved.

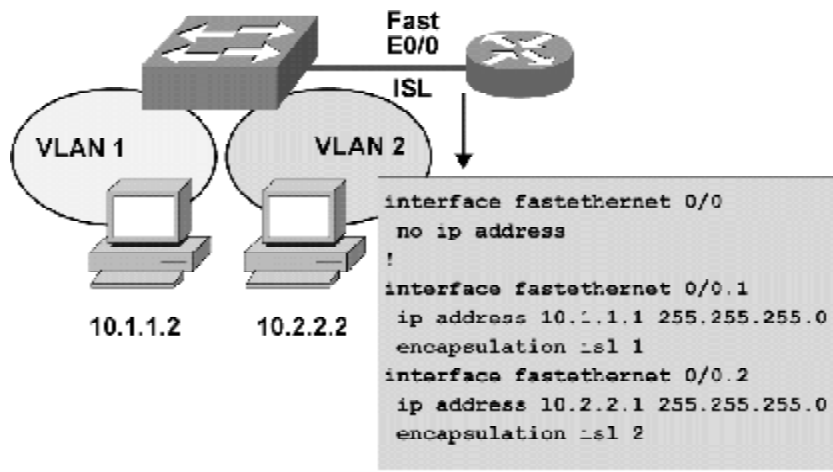
ICND v2.1—3-23

To support ISL or 802.1Q trunking, you must subdivide the physical Fast Ethernet interface of the router into multiple, logical, addressable interfaces, one per VLAN. The resulting logical interfaces are called subinterfaces. Without this subdivision, a separate physical interface would have to be dedicated to each VLAN.

In the figure, the FastEthernet0/0 interface is divided into multiple subinterfaces: FastEthernet0/0.1, FastEthernet0/0.2, and FastEthernet0/0.3.

Routing Between VLANs with ISL Trunks

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-24

Use the **encapsulation isl** *vlan identifier* subinterface configuration command to enable ISL on a router subinterface (where *vlan identifier* is the VLAN number).

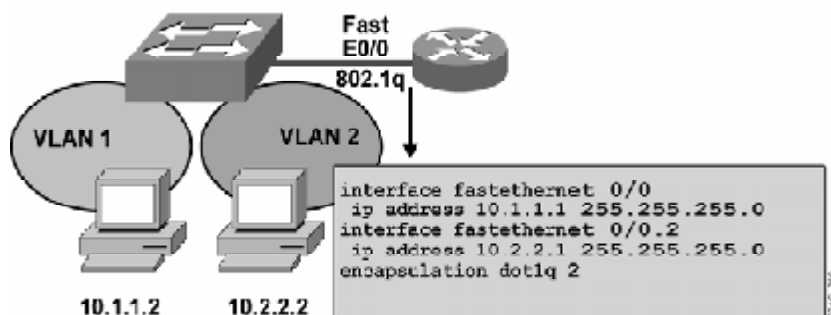
To configure the “router on a stick” for interVLAN routing, complete the following tasks:

1. Enable ISL on the switch port connecting to the router.
2. Enable ISL encapsulation on the router Fast Ethernet subinterface.
3. Assign a network layer address to each subinterface.

Note In this example, the VLANs are directly connected. Routing between networks not directly connected requires that the router learn the routes either statically or dynamically (such as via a routing protocol).

Routing Between VLANs with 802.1Q Trunks

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-25

Use the **switchport trunk encapsulation dot1q** subinterface configuration command to enable 802.1Q encapsulation trunking on a router subinterface.

802.1Q is slightly different from ISL. The native VLAN frames in 802.1Q do not carry a tag. Therefore, the major interface of a trunk has an address. Any other configuration information for the native VLAN subinterfaces is configured with the dot1Q encapsulation, IP address, and so on. The subinterface number need not equal the dot1Q VLAN number. However, management is easier when the two numbers are the same.

The Catalyst 2950 series switches support 802.1Q encapsulation only, which is configured automatically when trunking is enabled on the interface by using **switchport mode trunk** command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Routing is the process by which an item gets from one location to another. In networking, a router is the device used to route traffic.**
- **Routers can forward packets over static routes or dynamic routes, based on the router configuration.**
- **Static routes can be important if the Cisco IOS software cannot build a route to a particular destination. Static routes are also useful for specifying a “gateway of last resort” to which all unroutable packets will be sent.**
- **A default route is a special type of static route used for situations when the route from a source to a destination is not known or when it is unfeasible for the routing table to store sufficient information about the route.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-26

Summary (Cont.)

Cisco.com

- **When the static routing configuration is complete, use the show ip route command to verify the configuration.**
- **Dynamic routing relies on a routing protocol to disseminate knowledge. A routing protocol defines the set of rules used by a router when it communicates with neighboring routers.**
- **The ip classless command prevents a router from dropping a packet destined for an unknown subnet.**
- **In a VLAN environment, frames are only switched between ports within the same broadcast domain so a Layer 3 device is required to enable interVLAN communication. Use ISL or 802.1Q to enable trunking on a router subinterface.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-27

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which two items does a router need to know in order to route traffic? (Choose two.)
- A) the type of data being sent
 - B) the best path to the destination
 - C) the source address of the traffic
 - D) the destination address of the traffic
 - E) the destination router to be used for packet delivery
- Q2) What is the purpose of a routing table?
- A) to compare different paths to a destination
 - B) to tell the router which addresses arrive on which ports
 - C) to tell the router which complete path to use to reach a destination
 - D) to tell the router which port to use when forwarding addressed packets
- Q3) In which two ways do static routes differ from dynamic routes? (Choose two.)
- A) Static routes are manually configured; dynamic routes are learned via a routing protocol.
 - B) Dynamic routes are manually configured; static routes are learned via a routing protocol.
 - C) Both static routes and dynamic routes are automatically updated when there is a topology change.
 - D) Static routes allow precise control over the path that data takes; dynamic routes provide less control over the path taken.
 - E) Static routes are automatically updated when there is a topology change; dynamic routes require a change to the router configuration when there is a topology change.
- Q4) In what way are static and dynamic routes the same?
- A) Both are learned by manual configuration.
 - B) Both are updated automatically when there is a topology change.
 - C) Both require the router to send routing updates for maintaining the routing table.
 - D) Both tell the router how to forward packets to networks that are not directly connected.

- Q5) What does the command `ip route 172.16.5.0 255.255.255.0 10.1.1.1` specify?
- A) Both 172.16.5.0 and 10.1.1.1 use a mask of 255.255.255.0.
 - B) The router should use network 172.16.5.0 to get to address 10.1.1.1.
 - C) You want the router to trace a route to network 172.16.5.0 via 10.1.1.1.
 - D) The router should use address 10.1.1.1 to get to devices on subnet 172.16.5.0.
- Q6) What is the complete command to configure a static route with the following parameters:
- Destination network is 172.16.1.0
 - Subnet mask is 255.255.255.0
 - Next-hop router is 172.16.2.1
- A) **`ip route 172.16.1.0 255.255.255.0`**
 - B) **`ip route 172.16.1.0 255.255.255.0 172.16.2.1`**
 - C) **`ip route 172.16.2.1 255.255.255.0 172.16.1.0`**
 - D) **`ip route 172.16.1.0 172.16.2.1 255.255.255.0`**
- Q7) A default route _____.
- A) is used only if there is a routing protocol configured on a router
 - B) is used when the route to the destination is not explicitly known
 - C) is used only if there is no routing protocol configured on a router
 - D) is always used, even if there is a known explicit route to the destination
- Q8) Which command correctly configures a default route that points to 192.168.12.5 as the next hop router?
- A) **`ip route 0.0.0.0 192.168.12.5`**
 - B) **`ip route 192.168.12.5 0.0.0.0 0.0.0.0`**
 - C) **`ip route 0.0.0.0 0.0.0.0 192.168.12.5`**
 - D) **`ip route 0.0.0.0 192.168.12.5 0.0.0.0`**
- Q9) Which command displays information about static route configuration on a Cisco router?
- A) **`show ip route`**
 - B) **`show ip static`**
 - C) **`show ip route static`**
 - D) **`show static ip route`**

- Q10) What are two examples of dynamic routing protocols? (Choose two.)
- A) IP
 - B) IPX
 - C) RIP
 - D) ARP
 - E) OSPF
- Q11) Why does a Cisco router use the administrative distance?
- A) to determine how far away the destination is
 - B) to determine how far away the next hop router is
 - C) to weight the metric used by the source of the routing information
 - D) to rate the trustworthiness of the source of the routing information
- Q12) What does the **ip classless** command do?
- A) makes all classes of addresses into class C addresses
 - B) changes class A addresses to class B addresses, and changes class B addresses to class C addresses
 - C) ensures that if the router receives any packets for which it does not have an explicit route, it will send the packets to the default route
 - D) ensures that if the router receives any class A or class B packets for which it does not have an explicit route, it will send the packets to the default route
- Q13) At what level do you execute the **ip classless** command on a Cisco router?
- A) ROM monitor
 - B) privileged EXEC
 - C) global configuration
 - D) router configuration
- Q14) Why is router on a stick a necessary solution?
- A) because Layer 2 LAN switches can also operate at Layer 3
 - B) because routers cannot route packets between multiple VLANs
 - C) because Layer 2 LAN switches can only support a single VLAN
 - D) because Layer 2 LAN switches cannot switch frames between multiple VLANs
- Q15) Which command enables ISL trunking for VLAN 10 on the FastEthernet subinterface of a router?
- A) **router isl 10**
 - B) **network isl 10**
 - C) **network 10 isl**
 - D) **encapsulation isl 10**

Quiz Answer Key

- Q1) B, D
Relates to: Introducing Routing
- Q2) D
Relates to: Introducing Routing
- Q3) A, D
Relates to: Comparing Static and Dynamic Routes
- Q4) D
Relates to: Comparing Static and Dynamic Routes
- Q5) D
Relates to: Configuring Static Routes
- Q6) B
Relates to: Configuring Static Routes
- Q7) B
Relates to: Configuring Default Route Forwarding
- Q8) C
Relates to: Configuring Default Route Forwarding
- Q9) A
Relates to: Verifying the Static Routing Configuration
- Q10) C, E
Relates to: Introducing Dynamic Routing Protocols
- Q11) D
Relates to: Introducing Dynamic Routing Protocols
- Q12) C
Relates to: Using the ip classless Command
- Q13) C
Relates to: Using the ip classless Command
- Q14) D
Relates to: InterVLAN Routing
- Q15) D
Relates to: InterVLAN Routing

Distance Vector Routing

Overview

Distance vector routing algorithms (also known as Bellman-Ford routing algorithms) call for each router to send all or some portion of its routing table to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. This lesson describes the operation of distance vector routing protocols.

Relevance

Understanding the operation of distance vector routing is critical to being able to enable, verify, and troubleshoot a distance vector routing protocol.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features offered by distance vector routing protocols and give examples of each
- Describe the issues associated with distance vector routing and identify solutions to those issues

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

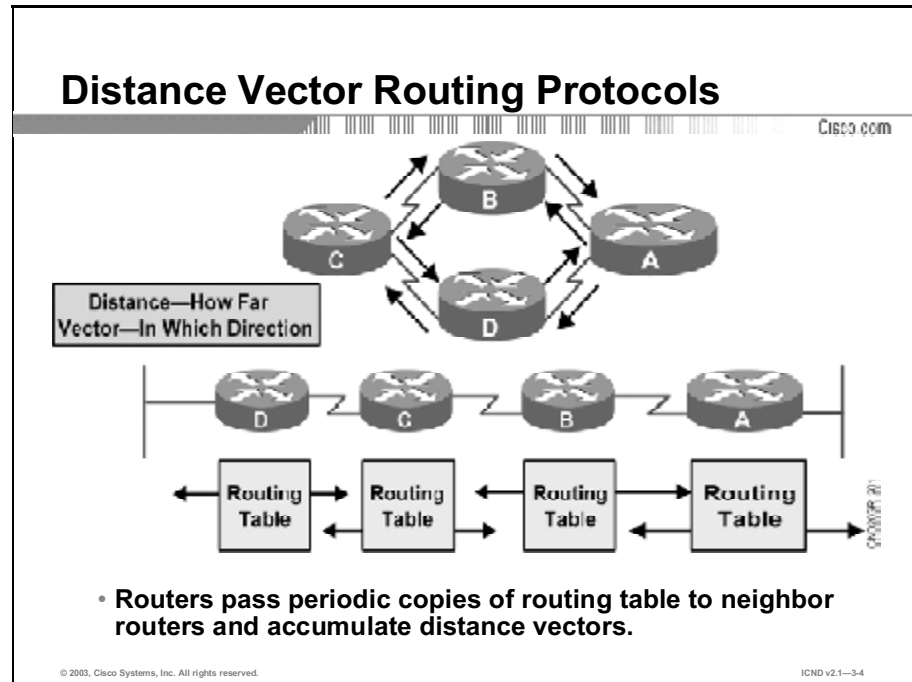
Outline

The lesson includes these topics:

- Overview
- Selecting Distance Vector Routes
- Maintaining Routing Information
- How Routing Inconsistencies Occur with Distance Vector Routing Protocols
- Defining a Maximum to Prevent Count to Infinity
- Solutions to Eliminate Routing Loops
- Distance Vector Operations
- Summary
- Quiz

Selecting Distance Vector Routes

Distance vector routing algorithms (also known as Bellman-Ford algorithms) pass periodic copies of a routing table from router to router. This topic describes how distance vector routing protocols operate.



The periodic routing updates that most distance vector routing protocols generate are only addressed to directly connected routing devices. The addressing scheme most commonly used is a logical broadcast. Routers running a distance vector routing protocol send periodic updates even if there are no changes in the network.

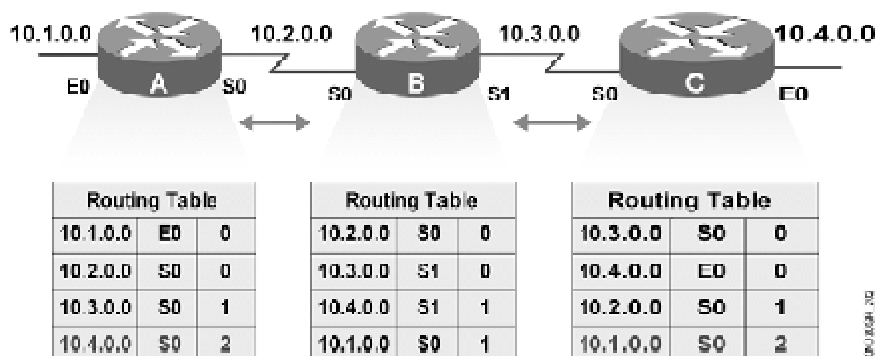
In a pure distance vector environment, the periodic routing update includes a complete routing table. By receiving a neighbor full routing table, a router can verify all known routes and make changes to the local routing table based on updated information. This process is also known as “routing by rumor,” because the router understanding of the network is based on the neighbor perspective of the network topology.

For example, in the figure, router B receives periodic routing updates from router A. Router B adds a distance vector metric (such as hop count) to each route learned from router A, increasing the distance vector. It then passes its own routing table to its neighbor, router C. This step-by-step process occurs in all directions between directly connected neighbor routers.

Traditionally, distance vector protocols were also classful protocols. Routing Information Protocol (RIP) v2 and Enhanced Interior Gateway Routing Protocol (EIGRP), are examples of more advanced distance vector protocols that exhibit classless behavior. EIGRP also exhibits some link-state characteristics.

Sources of Information and Discovering Routes

Cisco.com



- Routers discover the best path to destinations from each neighbor.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

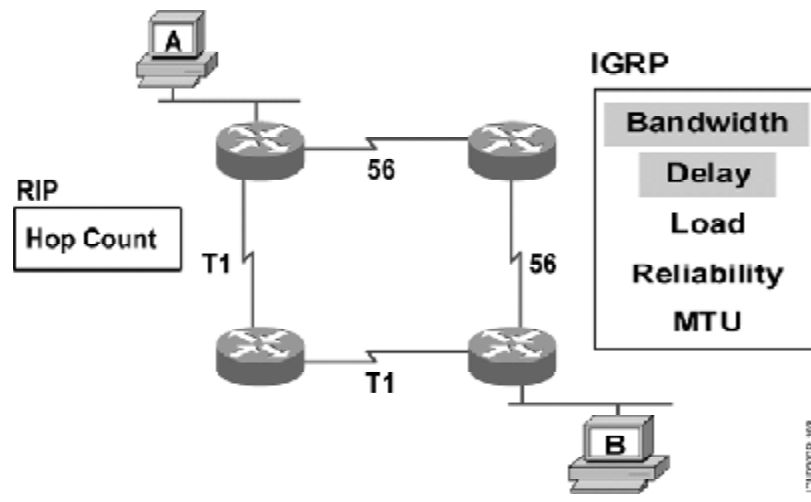
In the figure, the interface to each directly connected network is shown as having a distance of 0.

As the distance vector network discovery process proceeds, routers discover the best path to destination networks that are not directly connected based on accumulated metrics from each neighbor. Neighboring routers provide information for routes that are not directly connected.

For example, router A learns about other networks that are not directly connected (10.3.0.0 and 10.4.0.0) based on information it receives from router B. Each of these other network entries in the routing table has an accumulated distance vector to show how far away that network is in a given direction.

Selecting the Best Route with Metrics

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-6

Multiple routes to a destination can exist. When a routing protocol algorithm updates the routing table, its primary objective is to determine the best route to include in the table. Each distance vector routing protocol uses a different routing metric to determine the best route. The algorithm generates a number called the *metric value* for each path through the network. Typically, the smaller the metric, the better the path.

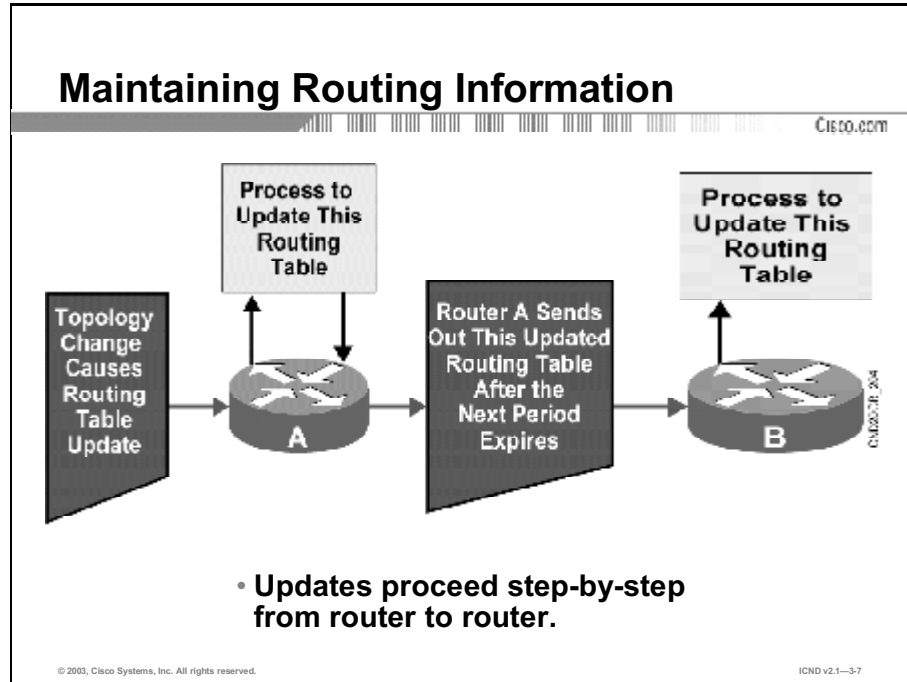
Metrics can be calculated based on a single characteristic of a path. More complex metrics can be calculated by combining several path characteristics. The metrics that distance vector routing protocols most commonly use are as follows:

- **Hop count:** Number of passages of a packet through the output port of one router.
- **Bandwidth:** Data capacity of a link. For instance, normally, a 10-Mbps Ethernet link is preferable to a 64-kbps leased line.
- **Delay:** Length of time required to move a packet from source to destination.
- **Load:** Amount of activity on a network resource such as a router or link.
- **Reliability:** Usually refers to the bit error rate of each network link.
- **Maximum transmission unit (MTU):** The maximum message length in octets that is acceptable to all links on the path.

For example, both RIP and Interior Gateway Routing Protocol (IGRP) are distance vector routing protocols. RIP uses hop count as the metric and IGRP uses a more advanced composite metric, which uses bandwidth and delay by default.

Maintaining Routing Information

When the topology of the internetwork changes, routing table updates must occur. Similar to the network discovery process, topology change updates proceed step-by-step from router to router. This topic explains how distance vector routing protocols maintain routing information.



Distance vector algorithms call for each router to send its entire routing table to each of its adjacent neighbors. Distance vector routing updates are sent periodically at regular intervals and the routing table can be sent immediately when the router detects a topology change using trigger updates.

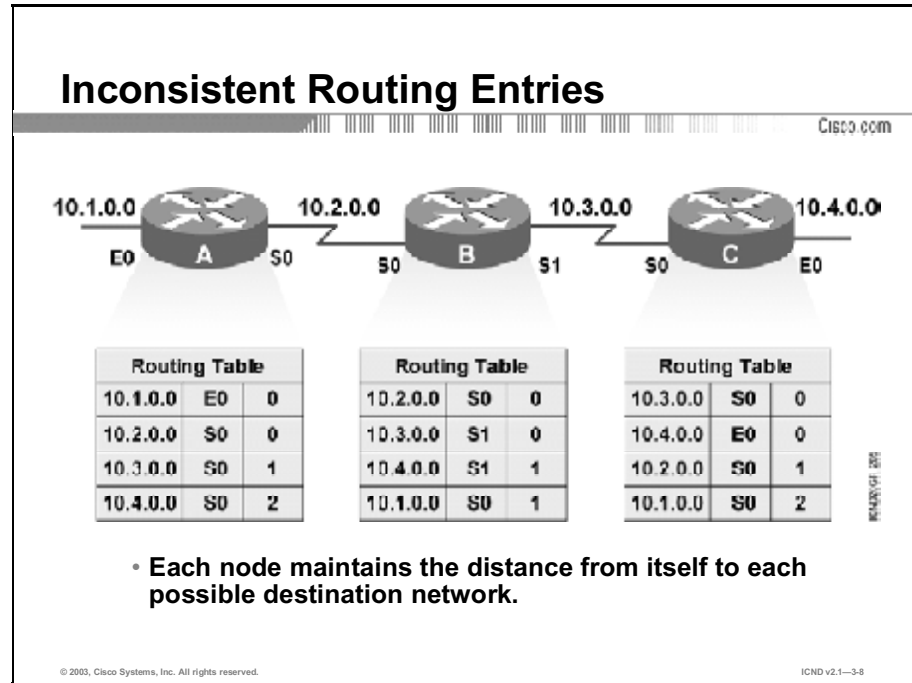
When a router receives an update from a neighboring router, it compares the update with its own routing table. The router adds the cost of reaching the neighbor router to the path cost reported by the neighbor to establish the new metric. If it learns about a better route (smaller total metric) to a network from its neighbor, the router updates its own routing table.

For example, if router B in the graphic is one unit of cost from router A, router B would add 1 to all costs reported by router A when router B runs the distance vector processes to update its routing table.

Each routing table entry includes information about the total path cost (defined by its metric) and the logical address of the first router on the path to each network it knows about.

How Routing Inconsistencies Occur with Distance Vector Routing Protocols

When maintaining the routing information, inconsistencies can occur if the slow internetwork convergence on a new configuration causes incorrect routing entries. This topic explains how routing inconsistencies occur with distance vector routing protocols.

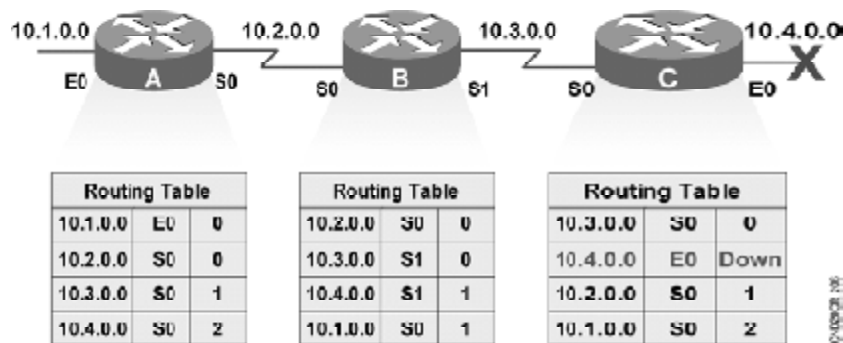


The example presented here uses a simplistic network design to convey the concepts.

- Just before the failure of network 10.4.0.0, all routers have consistent knowledge and correct routing tables. The network is said to have *converged*. Router C is directly connected to network 10.4.0.0 with a distance of 0 (hop). The router A path to network 10.4.0.0 is through router B, with a hop count of 2.

Inconsistent Routing Entries (Cont.)

Cisco.com



- Slow convergence produces inconsistent routing.

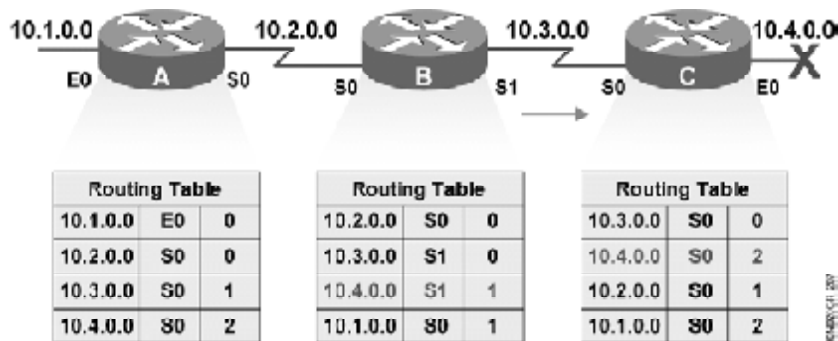
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-9

- When network 10.4.0.0 fails, router C detects the failure and stops routing packets out its E0 interface. However, routers A and B have not yet received notification of the failure. Router A still believes it can access 10.4.0.0 through router B. The router A routing table still reflects a path to network 10.4.0.0 with a distance of 2.

Inconsistent Routing Entries (Cont.)

Cisco.com



- Router C concludes that the best path to network 10.4.0.0 is through router B.

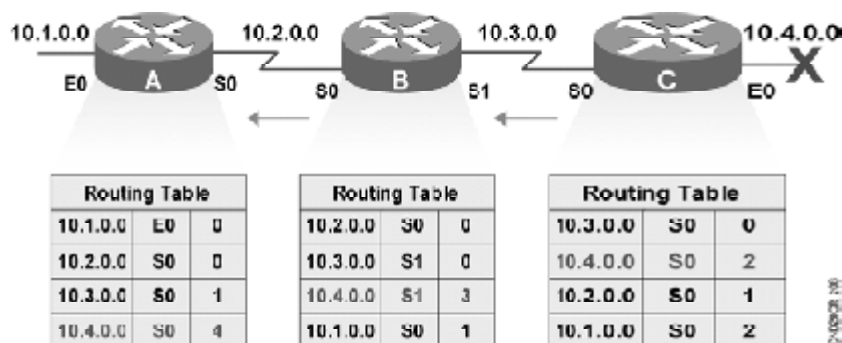
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-10

- When router B sends its periodic copy of its routing table to router C, router C believes it now has a viable path to network 10.4.0.0 through router B. Router C updates its routing table to reflect a path to network 10.4.0.0 through router B with a hop count of 2.

Inconsistent Routing Entries (Cont.)

Cisco.com



- Router A updates its table to reflect the new but erroneous hop count.

© 2003, Cisco Systems, Inc. All rights reserved.

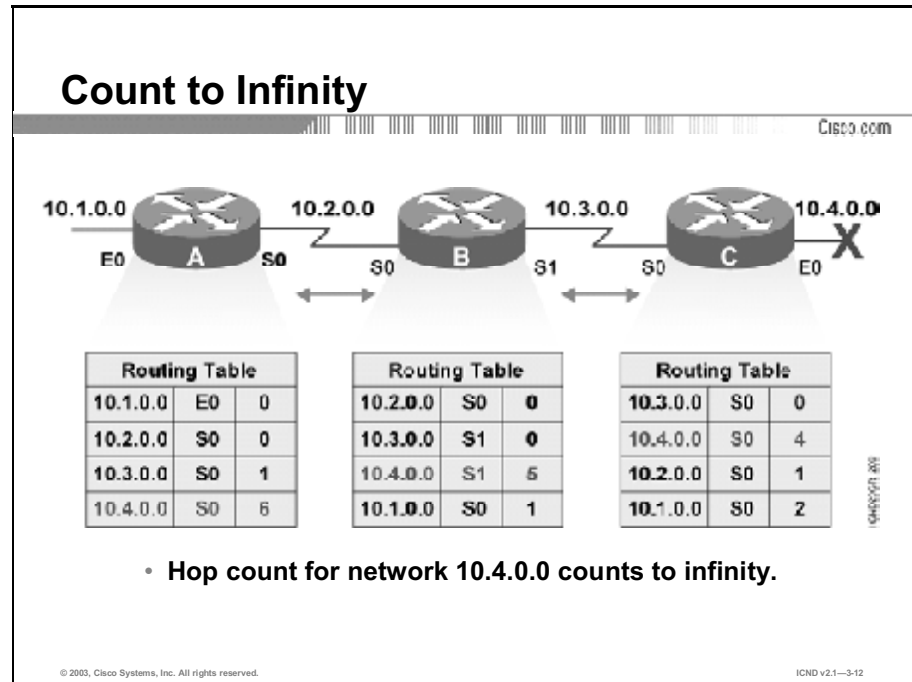
ICND v2.1—3-11

- Router B receives a new update from router C and updates its own table to reflect the new cost (3 hops). Router A receives the new routing table from router B, detects the modified distance vector to network 10.4.0.0, and recalculates its own distance vector to 10.4.0.0 as 4.

At this point, the routing tables of all three routers are incorrect, showing that network 10.4.0.0 can be reached by paths that do not exist, with hop counts that are meaningless. Routing table updates will continue to be sent out with the hop count growing ever larger (a problem called *count to infinity*). Additionally, packets destined for network 10.4.0.0 will never reach their destination, but rather bounce continuously between the routers (a routing *loop*).

Defining a Maximum to Prevent Count to Infinity

The condition called *count to infinity* arises when routing table updates continue to increase the metric to a destination that cannot be reached, rather than marking the destination as unreachable. This topic describes the problem of count to infinity and presents the solution.



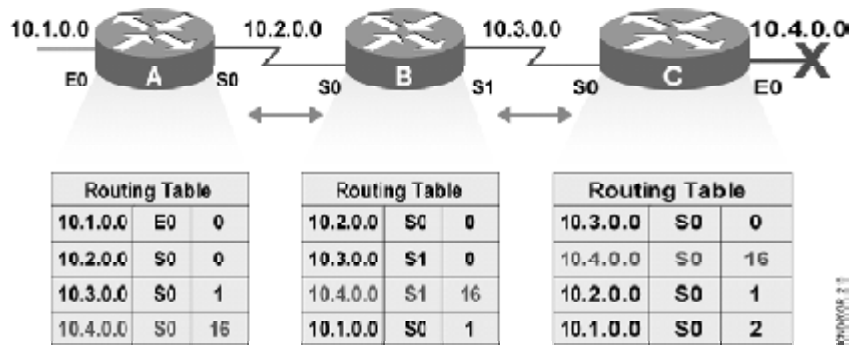
Continuing from the previous example, the invalid updates about network 10.4.0.0 continue to be propagated. Until some other process can stop the looping, the routers update each other in an inappropriate way, failing to consider the fact that network 10.4.0.0 is down.

This condition, called count to infinity, continuously updates the hop count metric, despite the fundamental fact that the destination network 10.4.0.0 is down. While the routers are counting to infinity, the invalid information (that a valid path to 10.4.0.0 exists) allows a routing loop.

Without countermeasures to stop the process, the hop-count distance vector increments each time a routing table update is passed to another router. These updates continue to proliferate because the destination is never marked as unreachable.

Defining a Maximum

Cisco.com



- Define a limit on the number of hops to prevent infinite loops.

© 2003, Cisco Systems, Inc. All rights reserved.

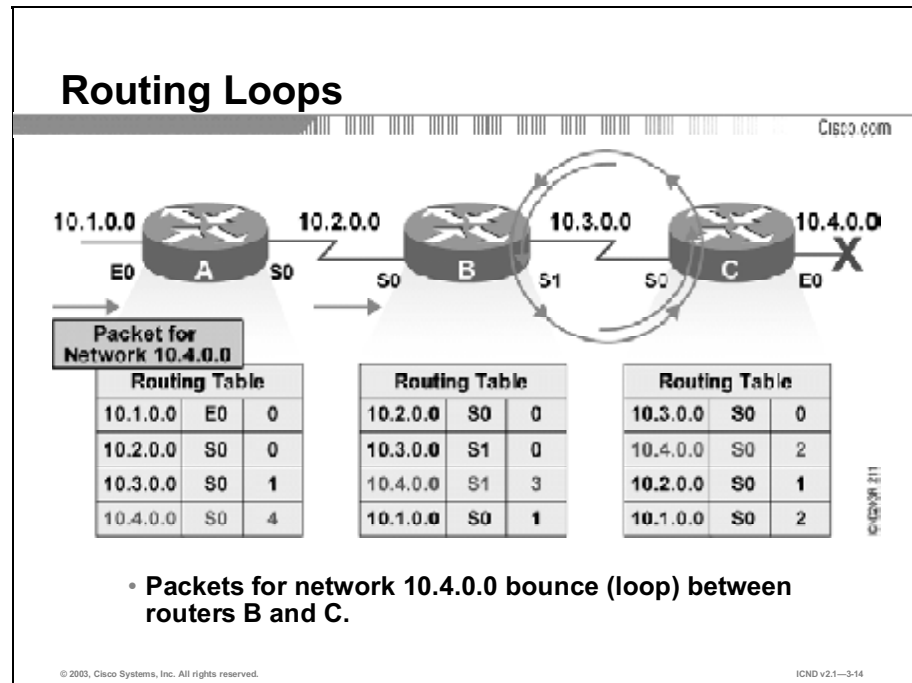
ICND v2.1—3-13

Distance vector protocols define infinity as some maximum number. This number refers to a routing metric, such as a hop count.

With this approach, the routing protocol permits the routing table update loop until the metric exceeds its maximum allowed value. The figure shows this defined maximum allowed value as 16 hops. When the metric value exceeds the maximum allowed value, network 10.4.0.0 is considered unreachable, stopping the proliferation of routing updates that increase the metric.

Solutions to Eliminate Routing Loops

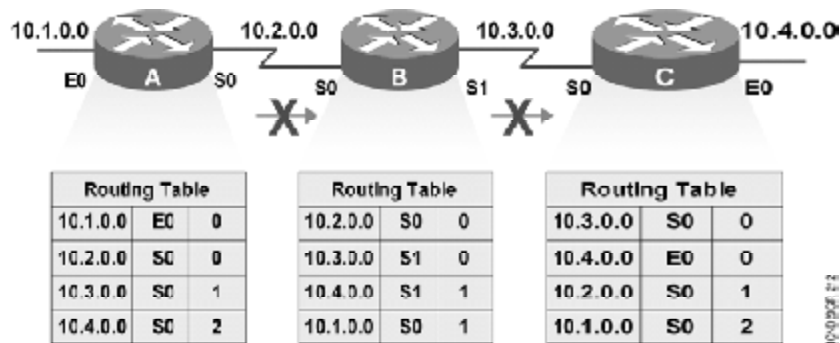
A routing loop occurs when two or more routers have incorrect routing information indicating that a valid path to an unreachable destination exists through the other routers. A number of techniques are available to eliminate routing loops, including split horizon, route poisoning, poison reverse, holddown timers, and triggered updates. This topic explains each technique to eliminate routing loops on distance vector routing networks.



In the example, a packet destined for network 10.4.0.0 arrives at router A. Per its routing table, router A forwards the packet out interface S0. The packet arrives at router B, which forwards it out its interface S1, as indicated in the router B routing table. Router C receives that packet and checks its routing table, which specifies that the packet should be forwarded out router C interface S0. The packet thus arrives back at router B, which again forwards it to router C over interface S1. The packet loops between routers B and C indefinitely.

Split Horizon

Cisco.com



- It is never useful to send information about a route back in the direction from which the original information came.

© 2003, Cisco Systems, Inc. All rights reserved.

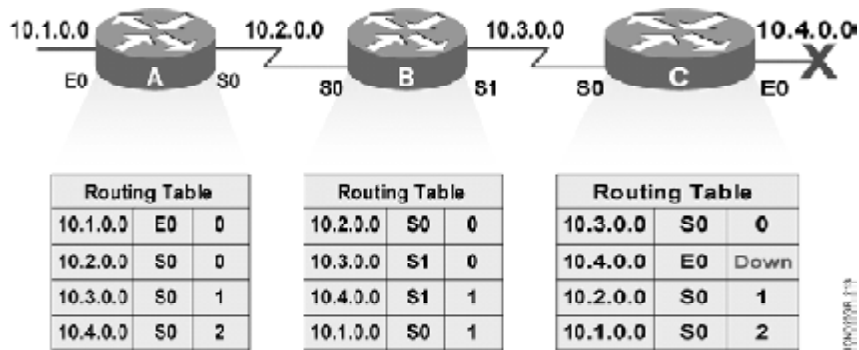
ICND v2.1—3-15

One way to eliminate routing loops and speed up convergence is through the technique called *split horizon*. The rule of split horizon is that it is never useful to send information about a route back in the direction from which the original information came. The following applies to the example:

- Router B has access to network 10.4.0.0 through router C. It makes no sense for router B to announce to router C that router B has access to network 10.4.0.0 through router C.
- Given that router B passed the announcement of its route to network 10.4.0.0 to router A, it makes no sense for router A to announce its distance from network 10.4.0.0 to router B.
- When router C announces that its connection to network 10.4.0.0 is down, router B sees that it has no alternative path to network 10.4.0.0, and concludes that network 10.4.0.0 is inaccessible, and router C will not incorrectly use router B to try to reach network 10.4.0.0.

Route Poisoning

Cisco.com



- Routers advertise the distance of routes that have gone down to infinity.

© 2003, Cisco Systems, Inc. All rights reserved.

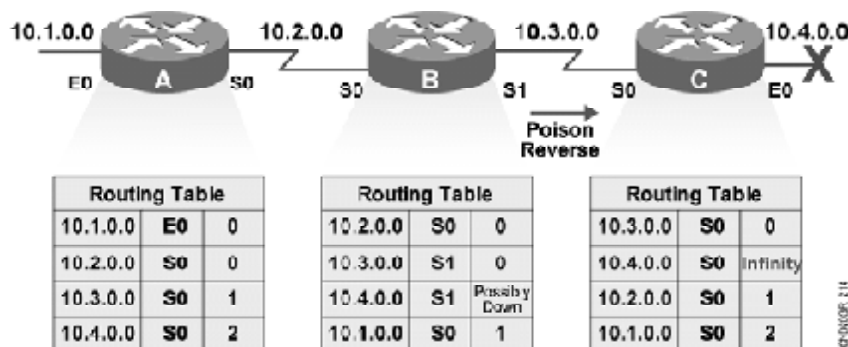
ICND v2.1—3-16

Another form of split horizon employs a technique called *route poisoning*. Route poisoning attempts to eliminate routing loops that are caused by inconsistent updates. With this technique, the router sets a table entry that keeps the network state consistent while other routers gradually converge correctly on the topology change. Used with holddown timers, route poisoning is a solution to long loops.

The figure provides an example. When network 10.4.0.0 goes down, router C poisons its link to network 10.4.0.0 by sending an update for that link as having infinite metric, hop count of 16 (that is, being unreachable). By poisoning its route to network 10.4.0.0, router C is not susceptible to incorrect updates about network 10.4.0.0 coming from neighboring routers that might claim to have a valid alternate path.

Poison Reverse

Cisco.com



- Poison reverse overrides split horizon.

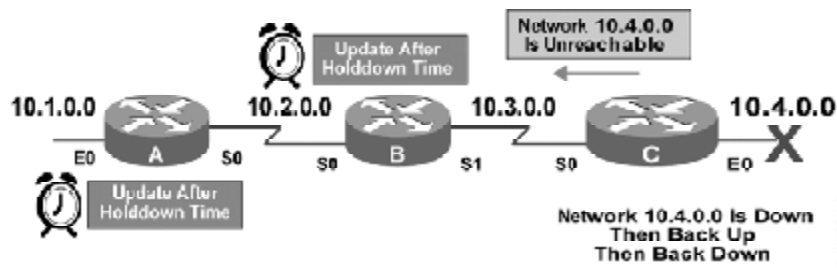
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-17

Split horizon with poison reverse improves convergence. When router B sees the metric to 10.4.0.0 jump to infinity, it sends an update called a *poison reverse* back to router C stating that network 10.4.0.0 is inaccessible. This is a specific circumstance overriding split horizon. This occurs to make sure router C is not susceptible to incorrect updates about network 10.4.0.0.

Holddown Timers

Cisco.com



- The router keeps an entry for the “possibly down state” in the network, allowing time for other routers to recompute for this topology change.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-18

Holddown timers are used to prevent regular update messages from inappropriately reinstating a route that may have gone bad. Holddowns tell routers to hold any changes that might affect routes for some period of time. The holddown period is set to three times the periodic update interval by default for RIP.

Holddown timers work as follows:

- When a router receives an update from a neighbor indicating that a previously accessible network is now inaccessible, the router marks the route as possibly down and starts a holddown timer.
- If an update arrives from a neighboring router with a better metric than originally recorded for the network, the router marks the network as accessible and removes the holddown timer.
- If at any time *before* the holddown timer expires an update is received from a different neighboring router with a poorer or same metric, the update is ignored. Ignoring an update with a poorer or same metric when a holddown is in effect allows more time for the knowledge of the change to propagate through the entire network.
- During the holddown period, routes appear in the routing table as “possibly down.” In the possibly down state, the router will still attempt to route packets to the possibly down network (maybe the network is just having intermediate connectivity problems, flapping up and down).

Triggered Updates

Cisco.com



- The router sends updates when a change in its routing table occurs.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-19

In the previous examples, routing loops were caused by erroneous information calculated as a result of inconsistent updates, slow convergence, and timing. If routers wait for their regularly scheduled updates before notifying neighboring routers of network changes, slow convergence problems can occur.

Normally, routing table updates are sent to neighboring routers on a regular interval. A triggered update is a routing table update that is sent immediately, in response to some change. The detecting router immediately sends an update message to adjacent routers that, in turn, generate triggered updates notifying their adjacent neighbors of the change. This wave will propagate throughout that portion of the network where routes went through the link.

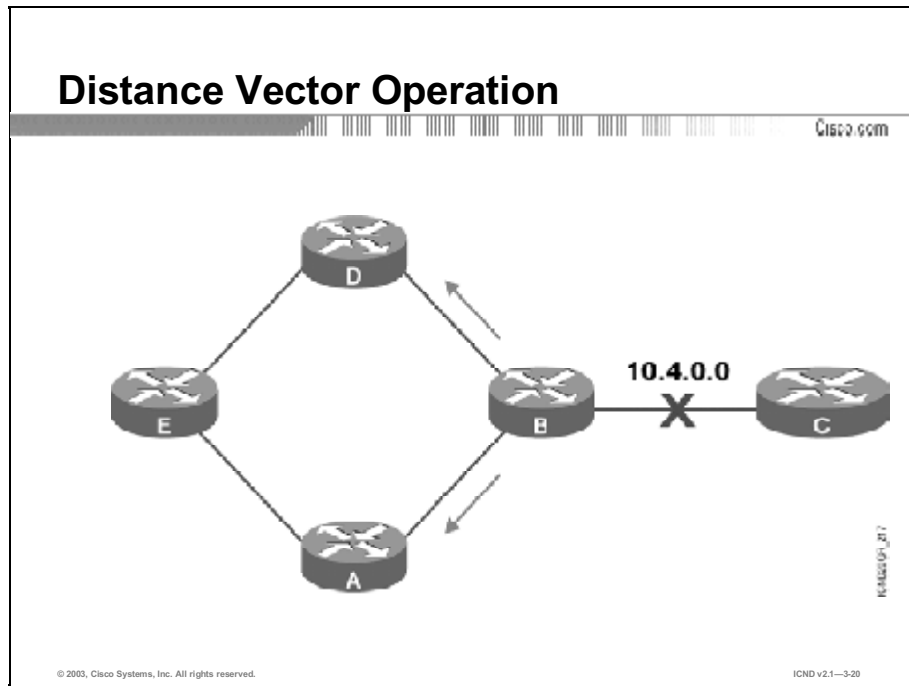
Triggered updates would be sufficient if there were a guarantee that the wave of updates reached every appropriate router immediately. However, there are two problems:

- Packets containing the update message can be dropped or corrupted by some link in the network.
- The triggered updates do not happen instantaneously. It is possible that a router that has not yet received the triggered update will issue a regular update at just the wrong time, causing the bad route to be reinserted in a neighbor that had already received the triggered update.

Coupling triggered updates with holddowns is designed to get around these problems. Because the holddown rule says that when a route is in holddown (possibly down), no new route with a same or worse metric will be accepted for the same destination for some period of time, so the triggered update has time to propagate throughout the network.

Distance Vector Operations

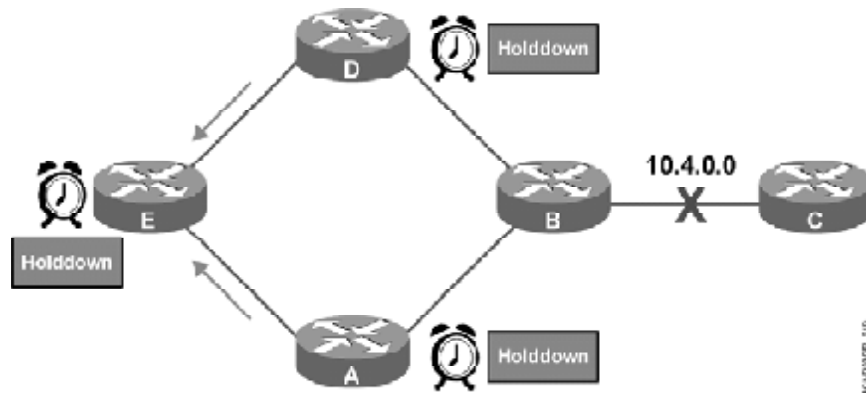
This topic provides an implementation example showing how to eliminate routing loops using split horizon, route poisoning, poison reverse, holddown timers, and triggered updates.



In the example, the routers A, B, D and E have multiple routes to reach network 10.4.0.0. As soon as router B detects the failure of network 10.4.0.0, router B removes its route to that network. Router B sends a trigger update to routers A and D, poisoning the route to network 10.4.0.0 by indicating an infinite metric to that network.

Distance Vector Operation (Cont.)

Cisco.com



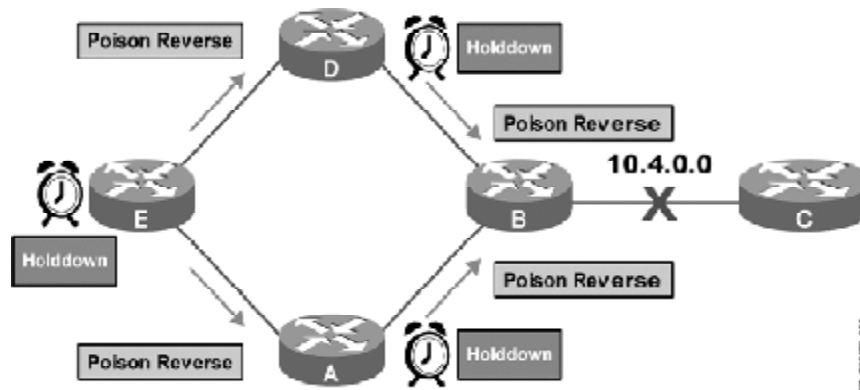
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-21

Routers D and A receive the triggered update and set their own holddown timers marking that the 10.4.0.0 network is possibly down. Routers D and A, in turn, send a triggered update to router E indicating the possible inaccessibility of network 10.4.0.0. Router E also sets the route to 10.4.0.0 in holddown.

Distance Vector Operation (Cont.)

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

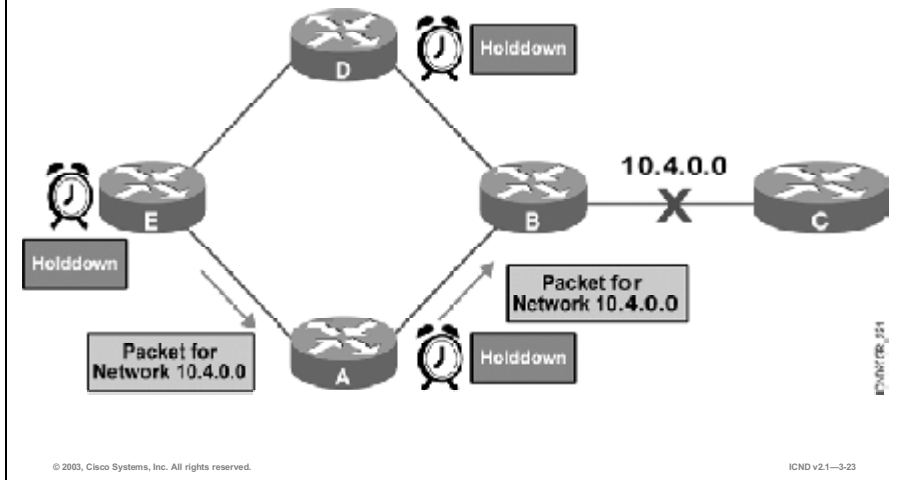
ICND v2.1—3-22

Routers A and D send a poison reverse to router B stating that network 10.4.0.0 is inaccessible.

Because router E received a triggered update from routers A and D, it sends a poison reverse to routers A and D also.

Distance Vector Operation (Cont.)

Cisco.com



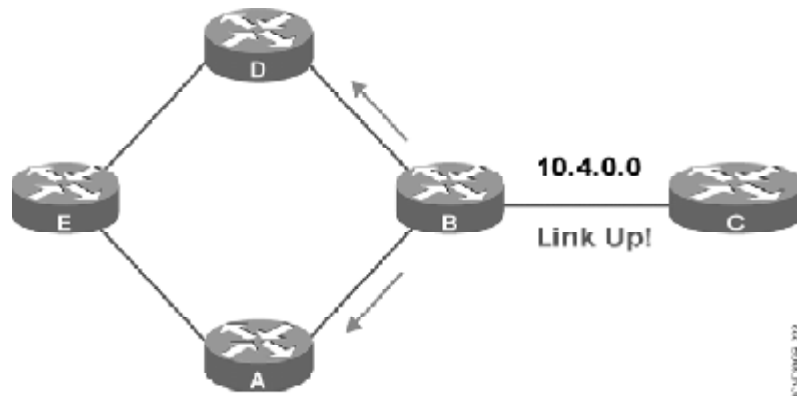
Routers A, D, and E will remain in holddown until either:

- The holddown timer expires
- Another update is received indicating a new route with a better metric
- A flush timer removes the route from the routing table

During the holddown period, routers A, D, and E assume that the network status is only possibly down and will attempt to route packets to network 10.4.0.0. The figure illustrates router E attempting to forward a packet to network 10.4.0.0. This packet will reach router B, but because router B has no route to network 10.4.0.0, router B will drop the packet and send back an Internet Message Control Protocol (ICMP) network unreachable message.

Distance Vector Operation (Cont.)

Cisco.com



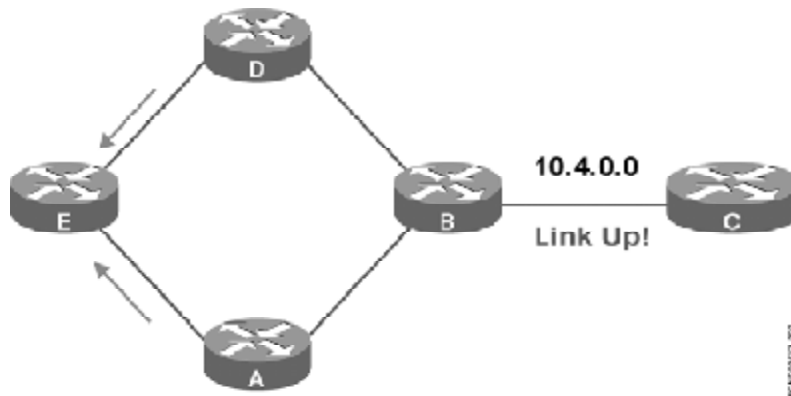
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-24

When the 10.4.0.0 network comes back up, router B will send a triggered update to routers A and D notifying them that the link is active. After the holddown timer expires, routers A and D change the route 10.4.0.0 from the possibly down state to the up state.

Distance Vector Operation (Cont.)

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-25

Routers A and D send router E a routing update stating that network 10.4.0.0 is up. Router E updates its routing table after the holddown timer expires.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Distance vector routing algorithms (also known as Bellman-Ford algorithms) pass periodic copies of a routing table from router to router.**
- **When the topology in a distance vector protocol internetwork changes, routing table updates must occur. As with the network discovery process, topology change updates proceed step-by-step from router to router.**
- **When maintaining the routing information, inconsistencies can occur if the slow convergence on a new configuration causes incorrect routing entries.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-26

Summary (Cont.)

Cisco.com

- **The condition called count to infinity arises when routing table updates continue to increase the metric to a destination that cannot be reached, rather than marking the destination as unreachable.**
- **A routing loop occurs when two or more routers have incorrect routing information indicating that a valid path to an unreachable destination exists through the other routers.**
- **A number of techniques are available to eliminate routing loops including: split horizon, route poisoning, poison reverse, holddown timers, and triggered updates.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-27

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) How does a distance vector router learn routing information?
- A) by creating a topology map of the entire network
 - B) by sending out regular poll messages to other routers
 - C) by listening to routing updates from all routers in the network
 - D) by listening to periodic routing updates from neighboring routers
- Q2) When a router receives distance vector information from a neighbor router, what does it do to the metric value of a given routing table entry?
- A) resets the metric value to 0
 - B) leaves the metric value as-is
 - C) increases the metric (such as hop count)
 - D) decreases the metric (such as hop count)
- Q3) Which two pieces of information are stored for each entry in a distance vector routing table? (Choose two.)
- A) total path cost
 - B) MAC address
 - C) address of last router in path to network
 - D) address of first router in path to network
 - E) address of each router in path to network
- Q4) What situation can cause routing inconsistencies?
- A) convergence
 - B) fast convergence
 - C) slow convergence
 - D) convergence interruption
- Q5) What is the problem called when routing inconsistencies cause packets sent to a particular destination to bounce continuously between routers?
- A) split horizon
 - B) a routing loop
 - C) a counting loop
 - D) a routing infinity

- Q6) What does a router do when a routing metric for a network exceeds the maximum?
- A) The router considers the network unreachable.
 - B) The router tries to find another path to that network.
 - C) The router sets the TTL value to something higher than the current maximum.
 - D) The router alerts the system administrator to change the maximum value of the metric.
- Q7) Count to infinity occurs when ____.
- A) routing table updates cause the distance vector metric to increment
 - B) routing table updates cause the distance vector metric to increment 15 times
 - C) routing table updates cause the distance vector metric to increment indefinitely
 - D) routing table updates cause the distance vector metric to decrement indefinitely
- Q8) What is the name of the rule that states “it is never useful to send information about a route back in the direction from which the original information came?”
- A) split horizon
 - B) poison reverse
 - C) route poisoning
 - D) defining a maximum
- Q9) Which solution to routing loops overrides split horizon?
- A) split horizon
 - B) poison reverse
 - C) route poisoning
 - D) defining a maximum
- Q10) While a router has a specific destination in holddown, what will it do with packets it receives for that destination?
- A) discard them
 - B) forward them as usual
 - C) forward them to the new route
 - D) forward them back to the sender
- Q11) Which two conditions will take a route out of holddown? (Choose two.)
- A) A flush timer removes the entry from the table.
 - B) A holddown timer removes the entry from the table.
 - C) An update arrives with a new route with a worst metric.
 - D) An update arrives with a new route with a better metric.
 - E) An update arrives with a new route with the same or better metric.

Quiz Answer Key

- Q1) D
Relates to: Selecting Distance Vector Routes
- Q2) C
Relates to: Selecting Distance Vector Routes
- Q3) A, D
Relates to: Maintaining Routing Information
- Q4) C
Relates to: How Routing Inconsistencies Occur in Distance Vector
- Q5) B
Relates to: How Routing Inconsistencies Occur in Distance Vector
- Q6) A
Relates to: Defining a Maximum to Prevent Count to Infinity
- Q7) C
Relates to: Defining a Maximum to Prevent Count to Infinity
- Q8) A
Relates to: Solutions to Eliminate Routing Loops
- Q9) B
Relates to: Solutions to Eliminate Routing Loops
- Q10) B
Relates to: Distance Vector Operations
- Q11) A, D
Relates to: Distance Vector Operations

Link-State and Balanced Hybrid Routing

Overview

Link-state routing algorithms, also known as shortest path first (SPF) algorithms, maintain a complex database of topology information. Whereas the distance vector algorithm has nonspecific information about distant networks and no knowledge of distant routers, a link-state routing algorithm maintains full knowledge of distant routers and how they interconnect. Balanced hybrid routing algorithms combine aspects of both distance vector and link state. This lesson explains both link-state and balanced hybrid routing algorithms.

Relevance

Understanding the operation of link-state routing protocols is critical to being able to enable, verify, and troubleshoot their operation.

Objectives

Upon completing this lesson, you will be able to:

- Describe the issues associated with link-state routing and identify solutions to those issues
- Describe the features of balanced hybrid routing protocols

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

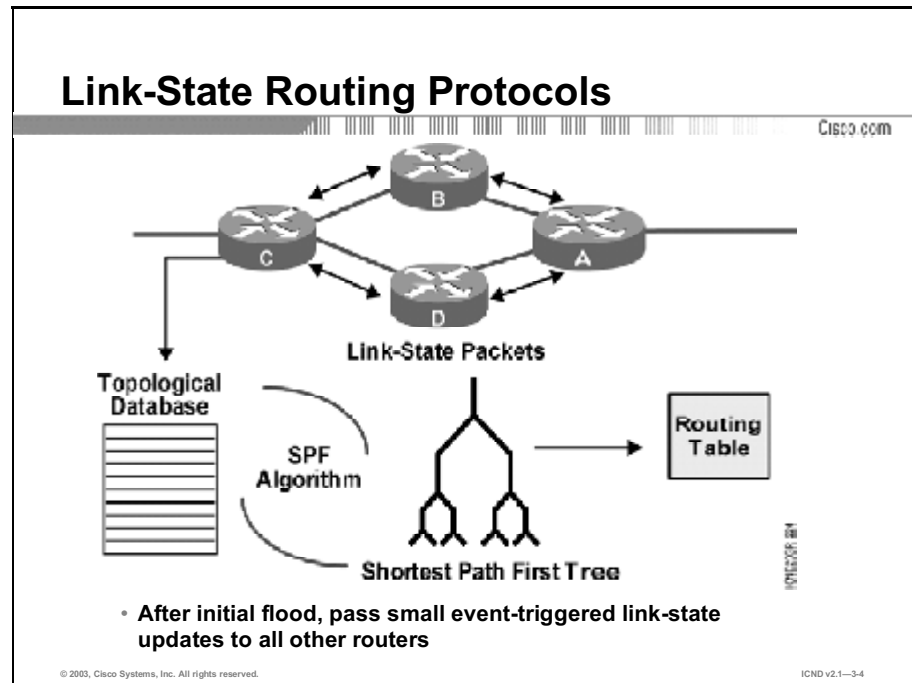
Outline

The lesson includes these topics:

- Overview
- How Routing Information Is Maintained with Link State
- Link-State Routing Protocol Algorithms
- Benefits and Drawbacks of Link-State Routing
- Balanced Hybrid Routing
- Summary
- Quiz

How Routing Information Is Maintained with Link State

Link-state routing uses link-state advertisements (LSAs), a topological database, the shortest path first (SPF) algorithm, the resulting SPF tree, and a routing table of paths and ports to each network. This topic describes how link-state protocols maintain routing information.



Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) Protocol are classified as link-state routing protocols. RFC 2328 describes OSPF link-state concepts and operations. Link-state routing protocols collect routing information from all other routers in the network or within a defined area of the network. After all of the information is collected, each router, independent of the other routers, calculates its best paths to all destinations in the network. Because each router maintains its own view of the network, it is less likely to propagate incorrect information provided by any one particular neighboring router.

Link-state routing protocols were designed to overcome the limitations of distance vector routing protocols. Link-state routing protocols respond quickly to network changes, send trigger updates only when a network change has occurred, and send periodic updates (known as *link-state refreshes*) at long time intervals, such as every 30 minutes. A “hello” mechanism determines the reachability of neighbors.

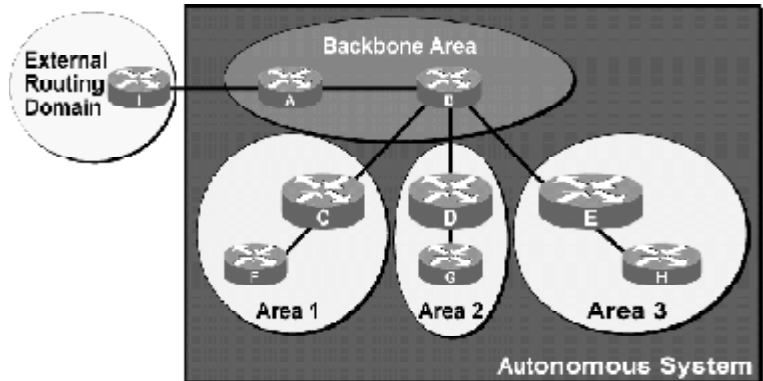
When a failure occurs in the network, such as a neighbor becomes unreachable, link-state protocols flood LSAs using a special multicast address throughout an area. Each link-state router takes a copy of the LSA, updates its link-state (topological) database, and forwards the LSA to all neighboring devices. LSAs cause every router within the area to recalculate routes. Because LSAs must be flooded throughout an area and all routers within that area must recalculate their routing tables, the number of link-state routers that can be in an area should be limited.

A link is similar to an interface on a router. The state of the link is a description of that interface and of its relationship to its neighboring routers. A description of the interface would include, for example, the IP address of the interface, the mask, the type of network to which it is connected, the routers connected to that network, and so on. The collection of link states forms a link-state, or topological, database. The link-state database is used to calculate the best paths through the network. Link-state routers find the best paths to destination by applying the Dijkstra SPF algorithm against the link-state database to build the SPF tree. The best paths are then selected from the SPF tree and placed in the routing table.

As networks become larger in scale, link-state routing protocols become more attractive for the following reasons:

- Link-state protocols send only updates of a topology change.
- Routing updates are more infrequent than for distance vector protocols.
- The network can be segmented into area hierarchies, limiting the scope of route changes.
- They support classless addressing.
- They send the subnet mask with the routing update.
- They support summarization.

Link-State Network Hierarchy Example



- Minimizes routing table entries
- Localizes impact of a topology change within an area

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

Link-state protocols use a two-layer network hierarchy. There are two primary elements in the two-layer network hierarchy:

- **Area:** An area is a grouping of contiguous networks. Areas are logical subdivisions of the autonomous system.
- **AS:** An AS consists of a collection of networks under a common administration that share a common routing strategy. An AS, sometimes called a domain, can be logically subdivided into multiple areas.

Within each AS, a contiguous backbone area must be defined. All other nonbackbone areas are connected off the backbone area. The backbone area is the transition area, because all other areas communicate through it. For OSPF, the nonbackbone areas can be additionally configured as a stub area, a totally stubby area, or a not-so-stubby area (NSSA) to help reduce the link-state database and routing table size.

Routers operating within the two-layer network hierarchy have different routing entities. The terms used to refer to these entities are different for OSPF than IS-IS. For example:

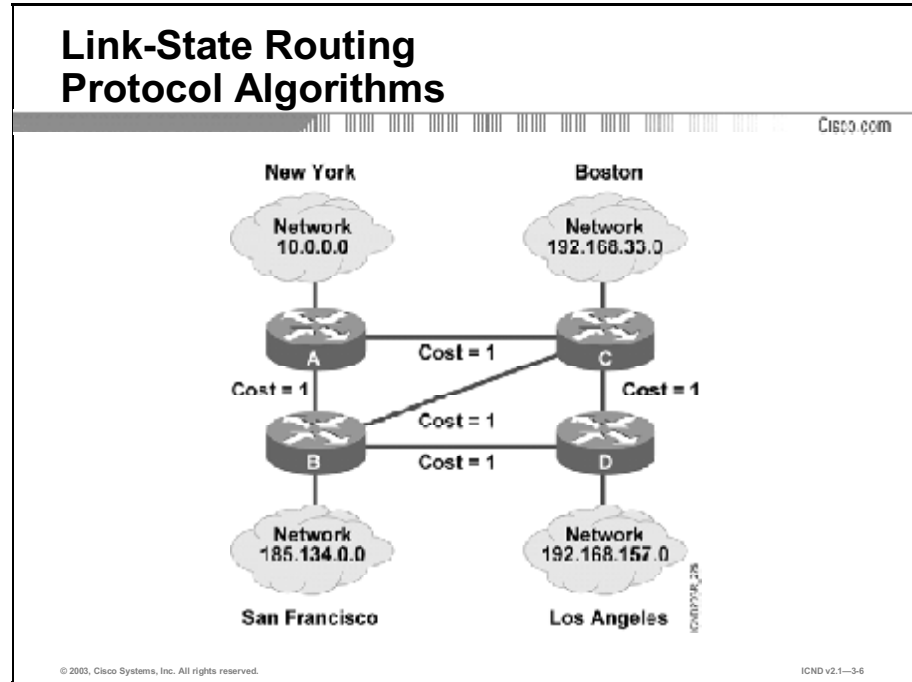
- Router B is called the backbone router in OSPF and the L2 router in IS-IS. The backbone, or L2 router, provides connectivity between different areas.
- Routers C, D, and E are called Area Border Routers (ABRs) in OSPF, and L1/L2 routers in IS-IS. ABR, or L1/L2, routers attach to multiple areas, maintain separate link-state databases for each area to which they are connected, and route traffic destined *for* or arriving *from* other areas.
- Routers F, G, and H are called nonbackbone internal routers in OSPF, or L1 routers in IS-IS. Nonbackbone internal, or L1 routers, are aware of the topology within their respective areas and maintain identical link-state databases about the areas.
- The ABR, or L1/L2 router, will advertise a default route to the nonbackbone internal, or L1 router. The nonbackbone internal, or L1 router, will use the default route to forward all interarea or interdomain traffic to the ABR, or L1/L2 router. This behavior can be different

for OSPF, depending on how the OSPF nonbackbone area is configured (stub area, totally stubby area, or NSSA).

- Router A is the autonomous system boundary router (ASBR) that connects to an external routing domain or an AS.
- Router I is a router that belongs to another routing domain (AS).

Link-State Routing Protocol Algorithms

Link-state routing algorithms maintain a complex database of the network topology by exchanging LSAs with other routers in a network. This topic describes the link-state routing algorithm.



Link-state routing algorithms, known collectively as SPF protocols, maintain a complex database of the network topology. Unlike distance vector protocols, link-state protocols develop and maintain a full knowledge of the network routers as well as how they interconnect. This is achieved through the exchange of LSAs with other routers in a network.

Each router that has exchanged LSAs constructs a topological database using all received LSAs. An SPF algorithm is then used to compute reachability to networked destinations. This information is used to update the routing table. This process can discover changes in the network topology caused by component failure or network growth.

In fact, the LSA exchange is triggered by an event in the network, instead of running periodically. This can greatly speed up the convergence process because there is no need to wait for a series of timers to expire before the networked routers can begin to converge.

Example

If the network shown on the slide uses a link-state routing protocol, there would be no concern about connectivity between New York City and San Francisco. Depending on the actual protocol employed, and the metrics selected, it is highly likely that the routing protocol could discriminate between the two paths to the same destination and try to use the best one. The table summarizes the contents of the routing tables.

Router	Destination	Next Hop	Cost
A	185.134.0.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	185.134.0.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	185.134.0.0	B	1
D	192.168.33.0	C	1

As shown in the table routing entries for the New York (router A) to Los Angeles (router D) routes, a link-state protocol would remember both routes. Some link-state protocols can even provide a means by which to assess the performance capabilities of these two routes, and bias toward the better-performing one. If the better-performing path, such as the route through Boston (router C), experienced operational difficulties of any kind, including congestion or component failure, the link-state routing protocol would detect this change and begin forwarding packets through San Francisco (router B).

Benefits and Drawbacks of Link-State Routing

Link-state routing may flood the network with LSAs during initial topology discovery, and can be both memory- and processor-intensive. This topic describes the benefits of link-state routing, the caveats to consider when using it, and the potential problems.

Benefits of Link-State Routing

Cisco.com

- **Fast convergence: changes are reported immediately by the source affected.**
- **Robustness against routing loops:**
 - Routers know the topology.
 - Link-state packets are sequenced and acknowledged.
- **By careful (hierarchical) network design, you can utilize resources optimally.**

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—3-7

Following are some of the many benefits that link-state routing protocols have over the traditional distance vector algorithms, such as Routing Information Protocol (RIP) v1 or Interior Gateway Routing Protocol (IGRP):

- Link-state protocols use cost metrics to choose paths through the network. The cost metric reflects the capacity of the links on those paths.
- By using triggered, flooded updates, link-state protocols can immediately report changes in the network topology to all routers in the network. This immediate reporting generally leads to fast convergence times.
- Because each router has a complete and synchronized picture of the network, it is very difficult for routing loops to occur.
- Because LSAs are sequenced and aged, routers always use the most recent set of information on which to base their routing decisions.
- With careful network design, the link-state database sizes can be minimized, leading to smaller Dijkstra calculations and faster convergence.

When to Use Link-State Routing Protocols

The link-state approach to dynamic routing can be quite useful in networks of any size. In a well-designed network, a link-state routing protocol will enable your network to gracefully adapt to unexpected topological change. Using events, such as changes, to drive updates, rather than fixed-interval timers, enables convergence to begin that much more quickly after a topological change.

The overhead of the frequent, time-driven updates of a distance vector routing protocol are also avoided. This allows more bandwidth to be available for routing traffic rather than for network maintenance, provided you design your network properly.

A side benefit of the bandwidth efficiency of link-state routing protocols is that they facilitate network scalability better than either static routes or distance vector protocols. When compared to the limitations of static routes or distance vector protocols, it is easy to see that link-state routing is best in larger, more complicated networks, or in networks that must be highly scalable. It can be challenging to initially configure a link-state protocol in a large network, but it is well worth the effort in the long run.

Caveats of Link-State Routing

Cisco.com

- **Significant demands for resources:**
 - **Memory (three tables: adjacency, topology, forwarding)**
 - **CPU (Dijkstra's algorithm can be intensive, especially when a lot of instabilities are present.)**
- **Requires very strict network design (when more areas—area routing)**
- **Problems with partitioning of areas**
- **Configuration generally simple but can be complex when tuning various parameters and when the design is complex**
- **Troubleshooting easier than in distance vector routing**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

Link-state protocols also have some limitations as follows:

- Link-state protocols require a topology database, an adjacency database, and a forwarding database, in addition to the routing table. This can require a significant amount of memory in large or complex networks.
- Dijkstra's algorithm requires CPU cycles to calculate the best paths through the network. If the network is large or complex (that is, the Dijkstra calculation is complex), or if the network is unstable (that is, the Dijkstra calculation is running on a regular basis), link-state protocols can use a significant amount of CPU power.
- To avoid an excessive use of memory or CPU power, a strict hierarchical network design is required, dividing the network into smaller areas to reduce the size of the topology tables and the length of the Dijkstra calculation. However, this dividing can cause problems because areas must remain contiguous at all times. The routers in an area must always be capable of contacting and receiving LSAs from all other routers in their area. In a multiarea design, an area router must always have a path to the backbone or it will have no connectivity to the rest of the network. Additionally, the backbone area must remain contiguous at all times to avoid some areas becoming isolated (partitioned).
- The configuration of link-state networks is usually simple, provided that the underlying network architecture has been soundly designed. If the network design is complex, then the operation of the link-state protocol may have to be tuned to accommodate it.
- Troubleshooting is usually easier in link-state networks because every router has a complete copy of the network architecture, or at least of its own area of the network. However, interpreting the information stored in the topology, neighbor databases, and the routing table requires a good understanding of the concepts of link-state routing.
- Link-state protocols usually scale to larger networks than distance vector protocols, particularly the traditional distance vector protocols such as RIPv1 and IGRP.

Drawbacks to Link-State Routing Protocols

Cisco.com

- **Initial discovery may cause flooding.**
- **Memory- and processor-intensive.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-9

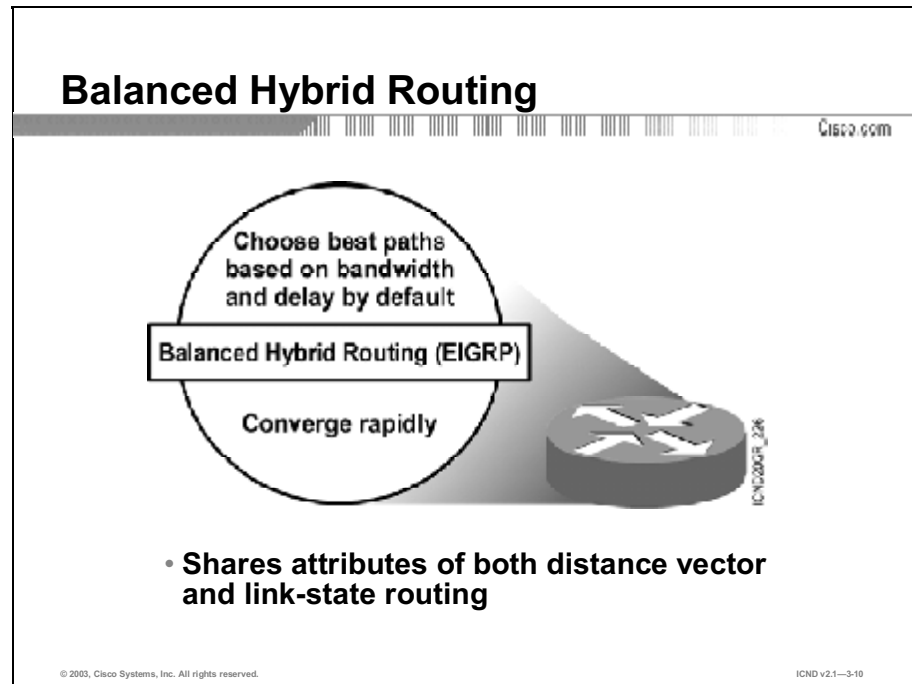
Despite all of its features and flexibility, link-state routing raises two potential concerns:

- During the initial discovery process, link-state routing protocols can flood the network with LSAs, and thereby significantly decrease the network capability to transport data. This performance compromise is temporary, but can be very noticeable. Whether this flooding process will noticeably degrade a network performance depends on two things: the amount of available bandwidth, and the number of routers that must exchange routing information. Flooding in large networks with relatively small links, such as low-bandwidth data-link connection identifiers (DLCIs) on a Frame Relay network, will be much more noticeable than a similar exercise on a small network with large-sized links, such as T3s.
- Link-state routing is both memory- and processor-intensive. Consequently, more fully configured routers are required to support link-state routing than distance vector routing. This increases the cost of the routers that are configured for link-state routing.

The potential performance impacts of both drawbacks can be addressed and resolved through foresight, planning, and engineering.

Balanced Hybrid Routing

Balanced hybrid routing protocols combine aspects of both distance vector and link-state protocols. This topic describes balanced hybrid routing.



The balanced hybrid routing protocol uses distance vectors with more accurate metrics to determine the best paths to destination networks. However, it differs from most distance vector protocols by using topology changes to trigger routing database updates as opposed to periodic updates.

The balanced hybrid routing type converges more rapidly than distance vectors, more like the link-state protocols. However, it differs from these protocols by emphasizing economy in the use of required resources such as bandwidth, memory, and processor overhead.

An example of a balanced hybrid protocol is the Cisco Enhanced Interior Gateway Routing Protocol (Enhanced IGRP or EIGRP).

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **Link-state routing uses LSAs, a topological database, the SPF algorithm, the resulting SPF tree, and a routing table of paths and ports to each network.**
- **Link-state routing algorithms maintain a complex database of the network topology by exchanging LSAs with other routers in a network.**
- **Link-state routing may flood the network with LSAs during initial topology discovery and can be both memory- and processor-intensive.**
- **Balanced hybrid routing protocols combine aspects of both distance vector and link-state protocols.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-11

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) How does a balanced hybrid routing protocol differ from a distance vector routing protocol?
- A) It uses link-state metrics.
 - B) It uses triggered updates.
 - C) It converges more slowly.
 - D) It only uses periodic updates.
- Q2) Which protocol is an example of a balanced hybrid protocol?
- A) RIP
 - B) IGRP
 - C) OSPF
 - D) EIGRP
- Q3) In a link-state protocol, what is the term used to describe a router interface and its relationship to neighboring routers?
- A) link
 - B) link state
 - C) link-state database
 - D) topological database
- Q4) Which protocol is an example of a link-state protocol?
- A) RIP
 - B) IGRP
 - C) OSPF
 - D) EIGRP
- Q5) How do link-state routers develop and maintain full knowledge of the network routers as well as how they interconnect?
- A) by exchanging links
 - B) by exchanging link states
 - C) by exchanging link-state databases
 - D) by exchanging link-state advertisements

- Q6) What process is greatly speeded up by the triggered exchange of LSAs?
- A) stability
 - B) notification
 - C) convergence
 - D) initial discovery
- Q7) During the initial discovery process, link-state routing protocols can flood the network with LSAs. What two factors determine if this flooding noticeably degrades performance? (Choose two.)
- A) available bandwidth
 - B) number of hops between routers
 - C) number of routers exchanging LSAs
 - D) number of links in link-state database
 - E) number of routers in network as a whole
- Q8) What are two advantages of link-state routing protocols over static routing or distance vector routing protocols? (Choose two.)
- A) timed updates
 - B) triggered updates
 - C) faster convergence
 - D) slower convergence
 - E) better in smaller, less complicated networks

Quiz Answer Key

- Q1) B
Relates to: How Routing Information Is Maintained with Link State
- Q2) C
Relates to: How Routing Information Is Maintained with Link State
- Q3) D
Relates to: Link-State Routing Protocol Algorithms
- Q4) C
Relates to: Link-State Routing Protocol Algorithms
- Q5) A, C
Relates to: Benefits and Drawbacks of Link-State Routing
- Q6) B, C
Relates to: Benefits and Drawbacks of Link-State Routing
- Q7) B
Relates to: Balanced Hybrid Routing
- Q8) D
Relates to: Balanced Hybrid Routing

Enabling RIP

Overview

The Routing Information Protocol (RIP) is one of the most enduring of all routing protocols. RIP is a relatively old, but still commonly used, interior gateway protocol created for use in small, homogeneous networks. It is a classical distance vector routing protocol. This lesson describes the basic RIP features and operation, and explains how to enable RIP on an IP network.

Relevance

While RIP is relatively old, it is still commonly used in IP networks. Knowing how to configure RIP is a key network administrator skill.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of RIP
- Use Cisco IOS commands to configure dynamic routing using RIP, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using RIP, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

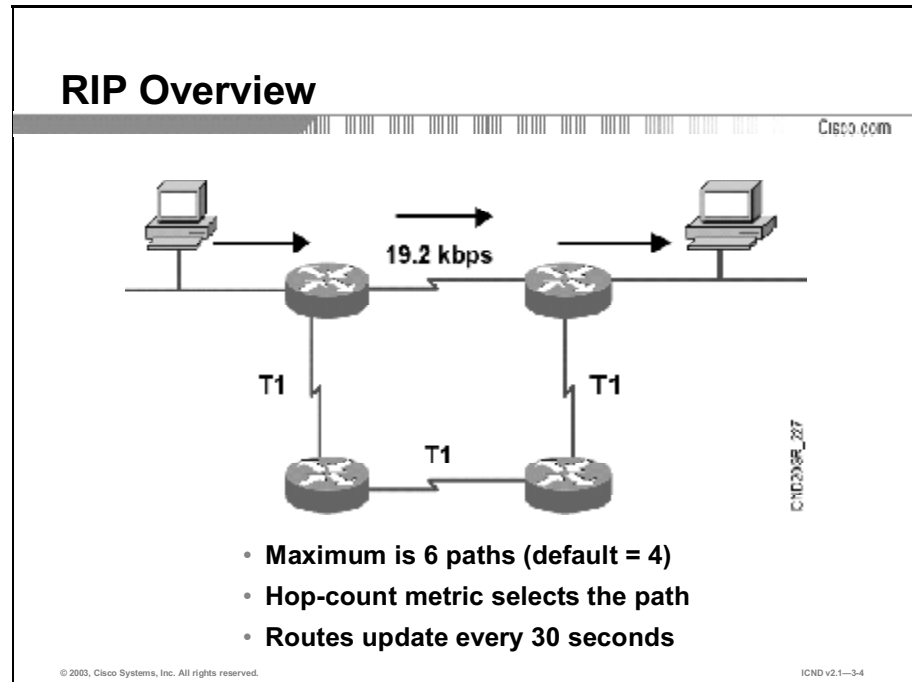
Outline

The lesson includes these topics:

- Overview
- RIP Features
- Configuring Dynamic Routing Protocols
- Configuring RIP
- Verifying the RIP Configuration
- Troubleshooting the RIP Configuration
- Summary
- Quiz

RIP Features

The Routing Information Protocol (RIP) is a distance vector routing protocol that uses hop count as the metric for route selection and broadcasts routing updates every 30 seconds. This topic describes RIP features.



RIP version 1 (RIPv1) is described in RFC 1058. An enhanced version, RIPv2, is a classless routing protocol that is defined in RFC 1721 and 1722.

Key characteristics of RIP include:

- It is a distance vector routing protocol.
- Hop count is used as the metric for path selection.
- The maximum allowable hop count is 15.
- Routing updates are broadcast every 30 seconds by default.
- RIP is capable of load-balancing over as many as six equal-cost paths. (Four paths is the default.)
- RIPv1 (classful routing protocol) does *not* send the subnet mask along with the routing update.
- RIPv2 (classless routing protocol) does send the subnet mask along with the routing update.

Defining the maximum number of parallel paths allowed in a routing table enables RIP load balancing. With RIP, the paths must be equal-cost paths. If the maximum number of paths is set to one, load balancing is disabled.

Note Cisco routers support RIPv1 and RIPv2. Here, you will learn how to enable RIPv1 only.

Configuring Dynamic Routing Protocols

To enable a dynamic routing protocol, you will select the routing protocol and then assign IP network numbers without specifying subnet values. This topic describes the basic commands that are used to configure a dynamic routing protocol on a Cisco router.

IP Routing Configuration Tasks

© 2003, Cisco Systems, Inc. All rights reserved.

- **Router configuration**
 - Select routing protocols
 - Specify networks or interfaces

Network 172.16.0.0

RIP

IGRP, RIP

Network 160.89.0.0

RIP

Network 172.30.0.0

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

To enable a dynamic routing protocol, the following tasks must be completed:

- Select a routing protocol such as RIP, Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), or Open Shortest Path First (OSPF).
- Assign IP network numbers without specifying subnet values (except for OSPF).

You must also assign network or subnet addresses and the appropriate subnet mask to the interfaces.

Dynamic routing uses broadcasts and multicasts to communicate with other routers.

The routing metric helps routers find the best path to each network or subnet.

Dynamic Routing Configuration

Cisco.com

```
Router(config)#router protocol [keyword]
```

- Defines an IP routing protocol

```
Router(config-router)#network network-number
```

- Mandatory configuration command for each IP routing process
- Identifies the physically connected network that routing updates are forwarded to

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-6

The **router** command starts a routing process.

router Command Parameters	Description
<i>protocol</i>	Either RIP, IGRP, OSPF, or EIGRP
<i>keyword</i>	Such as <i>autonomous system</i> , which is used with those protocols that require an autonomous system (IGRP and EIGRP). The keyword can also identify a local process ID, which is used with OSPF.

The **network** command is required because it allows the routing process to determine which interfaces will participate in the sending and receiving of the routing updates. The **network** command starts up the routing protocol on all interfaces that the router has in the specified network. The **network** command also allows the router to advertise that network.

network Command Parameter	Description
<i>network-number</i>	Specifies a directly connected network.

Configuring RIP

The **router rip** command specifies RIP as the routing protocol while the **network** command identifies a participating attached network. This topic describes how to configure basic RIP routing.

RIP Configuration



```
Router(config)#router rip
```

- Starts the RIP routing process

```
Router(config-router)#network network-number
```

- Selects participating attached networks
- Requires a major classful network number

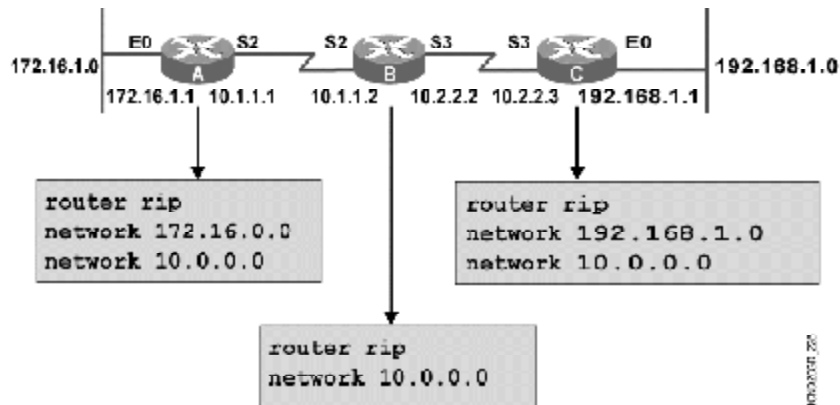
© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—37

The **router rip** command selects RIP as the routing protocol.

The **network** command assigns a major network number to which the router is directly connected. The RIP routing process will associate interface addresses with the advertised network number and will begin RIP packet processing on the specified interfaces.

RIP Configuration Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

In the example, the router A configuration includes the following:

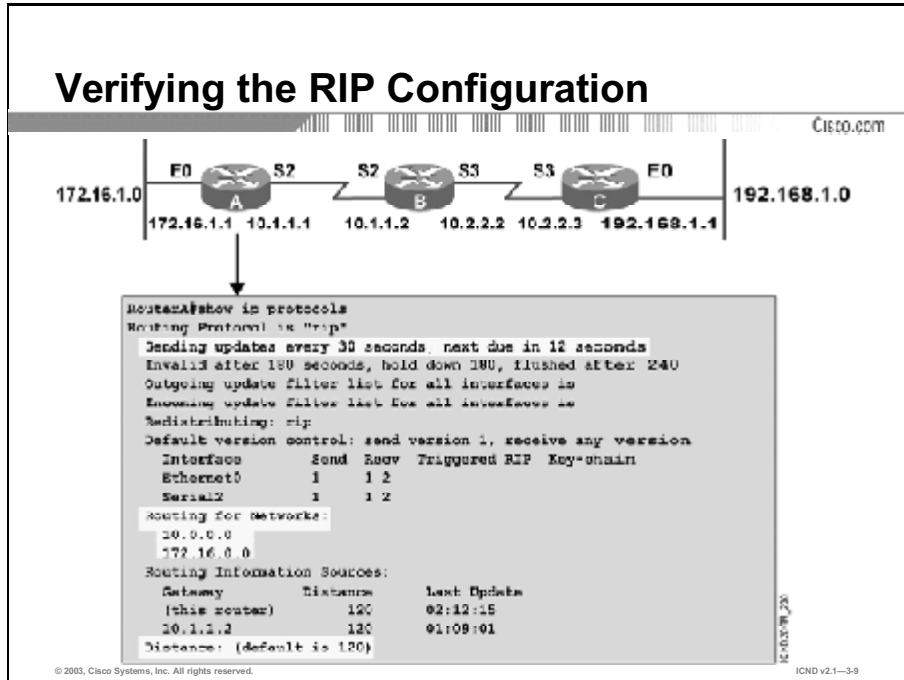
- **router rip:** Selects RIP as the routing protocol.
- **network 172.16.0.0:** Specifies a directly connected network.
- **network 10.0.0.0:** Specifies a directly connected network.

The router A interfaces that are connected to networks 172.16.0.0 and 10.0.0.0, or their subnets, will send and receive RIP updates. These routing updates allow the router to learn the network topology.

Routers B and C have similar RIP configurations but with different network numbers specified.

Verifying the RIP Configuration

The **show ip protocols** and **show ip route** commands display information about routing protocols and the routing table. This topic describes how to use **show** commands to verify the RIP configuration.



The **show ip protocols** command displays values about routing protocols and the routing protocol timer information that is associated with the router.

In the example, the router is configured with RIP and sends updated routing table information every 30 seconds. (This interval is configurable.) If a router running RIP does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being invalid. In the figure, the holddown timer is set to 180 seconds. As a result, an update to a route that was down and is now up will stay in holddown (possibly down) state until 180 seconds have passed.

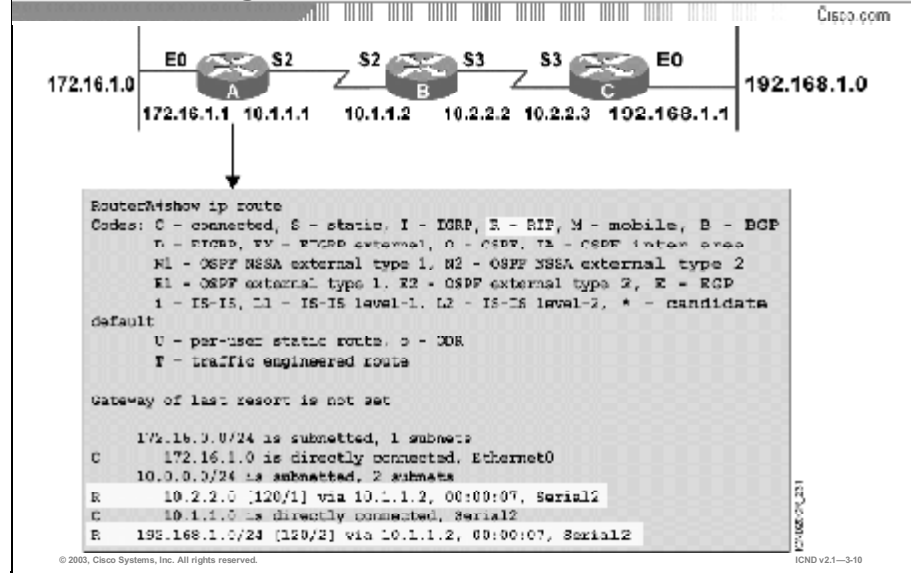
If there is still no update after 240 seconds (flush timer), the router removes the routing table entries from the router. In the figure, it has been 10 seconds since router A received an update from router B.

The router is injecting routes for the networks that are listed following the “Routing for Networks” line. The router is receiving routes from the neighboring RIP routers that are listed following the “Routing Information Sources” line.

The distance default of 120 refers to the administrative distance for an RIP route.

You can also use the **show ip interface brief** command to list a summary of interface IP information and status.

Displaying the IP Routing Table



The **show ip route** command displays the contents of the IP routing table.

The routing table contains entries for all known networks and subnetworks, and contains a code that indicates how that information was learned. The output of key fields from this command, and their function, is explained in the table.

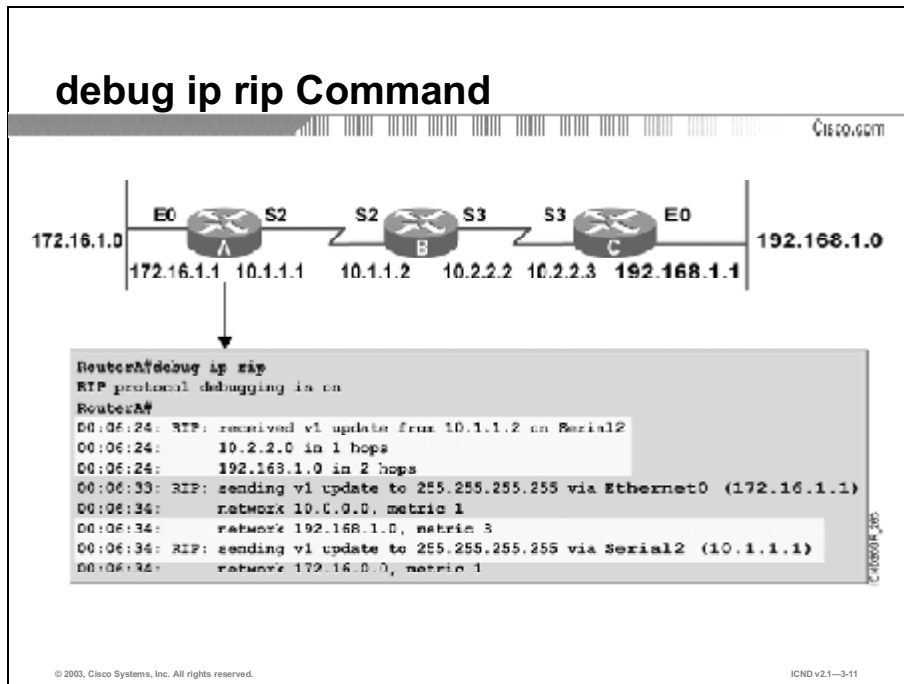
Output	Description
R or C	Identifies the source of the route. For example, a C indicates the route came from a direct connection of the route to a router interface. An R indicates RIP is the protocol that determined the route.
192.168.1.0 10.2.2.0	Indicates the address of the remote network.
120/1	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route (for example, 1 hop).
via 10.1.1.2	Specifies the address of the next hop router to the remote network.
00:00:07	Specifies the time since the route was updated in hours, minutes, seconds.
Serial2	Specifies the interface through which the specified network can be reached.

Examine the output to see if the routing table is populated with routing information.

If routing information is not being exchanged (that is, if the output of the **show ip route** command shows no entries that were learned from a routing protocol), use the **show running-config** or **show ip protocols** privileged EXEC commands on the router to check for a possible misconfigured routing protocol.

Troubleshooting the RIP Configuration

Use the **debug ip rip** EXEC command to display information on RIP routing transactions. This topic explains the use of the **debug ip rip** command.



Use the **debug ip rip** command to display RIP routing updates as they are sent and received. The **no debug all** command turns off all debugging.

The example shows that the router being debugged has received updates from one router at source address 10.1.1.2. That router sent information about two destinations in the routing table update. The router being debugged also sent updates, in both cases to broadcast address 255.255.255.255 as the destination. The number in parentheses is the source address that is encapsulated into the IP header.

Other output that you might see from the **debug ip rip** command includes entries such as the following:

```
RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1
```

Entries like these can appear at startup or when an event occurs, such as an interface transitioning or a user manually clearing the routing table.

The following entry is most likely caused by a malformed packet from the transmitter:

```
RIP: bad version 128 from 160.89.80.43
```


Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **RIP is a distance vector routing protocol that uses hop count as the metric for route selection and broadcasts routing updates every 30 seconds.**
- **To enable a dynamic routing protocol, you will select the routing protocol and then assign IP network numbers.**
- **The router rip command specifies RIP as the routing protocol. The network command identifies a participating attached network.**
- **The show ip commands display information about routing protocols and the routing table.**
- **Use the debug ip rip command to display information on RIP routing transactions.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-12

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What are two characteristics offered by RIPv1? (Choose two.)
- A) It is a link-state protocol.
 - B) It uses hop count as a metric.
 - C) It has a maximum hop count of 16.
 - D) It can load balance over six equal cost paths.
 - E) It broadcasts updates every 90 seconds by default.
- Q2) RIP can load balance over as many as _____ equal-cost paths, with _____ as the default.
- A) 6, 4
 - B) 6, 6
 - C) 8, 4
 - D) 8, 6
- Q3) On a Cisco router, which two functions does the **network** command perform? (Choose two.)
- A) allows the router to advertise the specified network
 - B) nothing, is an optional command when configuring RIP
 - C) starts up the routing protocol on all interfaces that the router has in the specified network
 - D) starts up the routing protocol on all interfaces that the router has in the specified subnets
- Q4) Which two things must be true about the network number assigned with the **network** command? (Choose two.)
- A) specifies the major network number
 - B) identifies the major network and subnetwork
 - C) includes the major network and the subnet mask
 - D) identifies a network the router can reach through other routers
 - E) identifies a network to which the router is physically connected

Q5) Router C has three interfaces as follows:

E0: 10.1.1.5

E1: 10.1.2.6

S0: 10.2.4.6

Which configuration is required to specify that RIP is to run on all of router C interfaces?

- A) network 10.0.0.0
- B) network 10.1.0.0, network 10.2.0.0
- C) network 10.1.1.0, network 10.1.2.0, network 10.2.4.0
- D) network 10.1.1.5, network 10.1.2.6, network 10.2.4.6

Q6) On a Cisco router, what two things does the **show ip protocols** command display? (Choose two.)

- A) interface information
- B) values of routing timers
- C) the contents of the routing table
- D) routing protocol information about the router as a whole

Q7) In the output of the **show ip route** command on a Cisco router, what information is displayed inside brackets?

- A) the next hop
- B) the address of the remote network
- C) the method used to learn the route
- D) the administrative distance and metric

Q8) Which message in the output of the **debug ip rip** command most likely indicates a malformed packet from the transmitter?

- A) RIP: bad version 128 from 160.89.80.43
- B) RIP: broadcasting general request on Ethernet0
- C) RIP: received v1 update from 10.1.1.1 on Ethernet 2
- D) RIP: sending v1 update to 255.255.255.255 via Ethernet 0

Q9) What would cause the message “RIP: broadcasting general request on Ethernet0” to be displayed in the output of the **debug ip rip** command?

- A) receiving a malformed packet
- B) sending a routing table update
- C) receiving a routing table update
- D) manually clearing the routing table

Quiz Answer Key

- Q1) B, D
Relates to: RIP Features
- Q2) A
Relates to: RIP Features
- Q3) A, C
Relates to: Configuring Dynamic Routing Protocols
- Q4) A, E
Relates to: Configuring Dynamic Routing Protocols
- Q5) A
Relates to: Configuring RIP
- Q6) B, D
Relates to: Verifying the RIP Configuration
- Q7) D
Relates to: Verifying the RIP Configuration
- Q8) A
Relates to: Troubleshooting the RIP Configuration
- Q9) D
Relates to: Troubleshooting the RIP Configuration

Enabling IGRP

Overview

The Interior Gateway Routing Protocol (IGRP) is a routing protocol that was developed in the mid-1980s by Cisco Systems. The principal goal in creating the Cisco IGRP was to provide a robust protocol for routing within an autonomous system. The popularity of Cisco routers and the robustness of IGRP encouraged many organizations with large internetworks to replace Routing Information Protocol (RIP) with IGRP. This lesson describes the features and operation of IGRP, and shows you how to configure its basic features.

Relevance

With the popularity of the Cisco IGRP protocol, you should know how to configure and maintain IGRP.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of IGRP
- Use Cisco IOS commands to configure dynamic routing using IGRP, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using IGRP, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

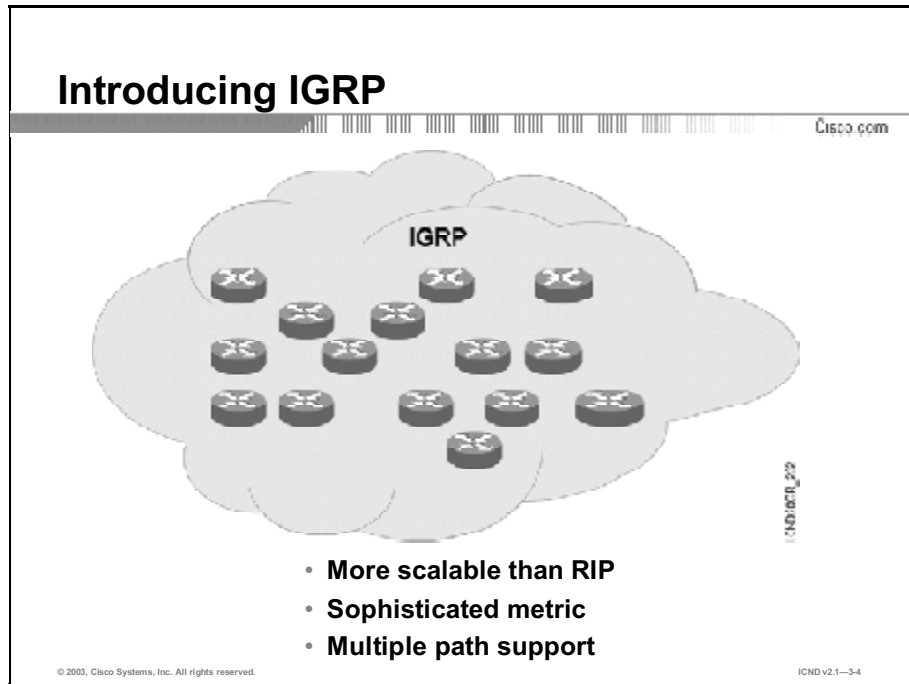
Outline

The lesson includes these topics:

- Overview
- IGRP Features
- IGRP Metrics
- Supporting Multiple Paths with IGRP
- Configuring IGRP
- Verifying the IGRP Configuration
- Troubleshooting the IGRP Configuration
- Summary
- Quiz

IGRP Features

The Interior Gateway Routing Protocol (IGRP) has several features that differentiate it from other distance vector routing protocols. These features include increased scalability, a sophisticated metric, and unequal-cost path load balancing. This topic describes the features of IGRP.



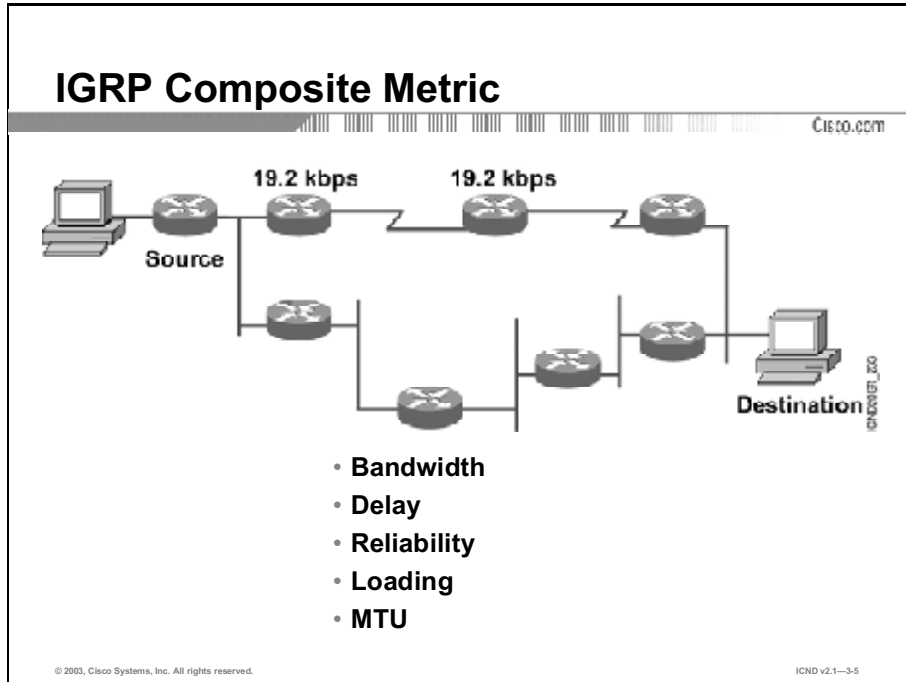
IGRP is an advanced distance vector routing protocol developed by Cisco in the mid-1980s. IGRP has several features that differentiate it from other distance vector routing protocols, such as Routing Information Protocol (RIP). These IGRP features are as follows:

- **Increased scalability:** Capable of routing in larger-sized networks compared with networks that use RIP.
- **Sophisticated metric:** IGRP uses a composite metric that provides significant route selection flexibility. Internetwork delay, bandwidth by default, load, and optional reliability are all factored into the routing decision. IGRP can be used to overcome the RIP 15-hop limit. IGRP has a default maximum hop count of 100 hops, configurable to a maximum of 255 hops.
- **Multiple paths:** IGRP can maintain up to six distinct paths between a network source and destination. The paths do not have equal costs as with RIP. Multiple paths can be used to increase available bandwidth or for route redundancy.

Use IGRP in IP networks that require a simple, robust, and more scalable routing protocol than RIP.

IGRP Metrics

IGRP uses a composite routing metric that can include bandwidth, delay, reliability, loading, and maximum transmission unit (MTU) values. This topic describes the components of the IGRP composite metric.



IGRP uses a composite routing metric. This combination metric provides greater accuracy than the RIP hop count metric when choosing a path to a destination. The path that has the smallest metric value is the best route. On Cisco IOS software, the IGRP metrics are weighted with the constants K1 through K5. These constants convert an IGRP metric vector into a scalar quantity.

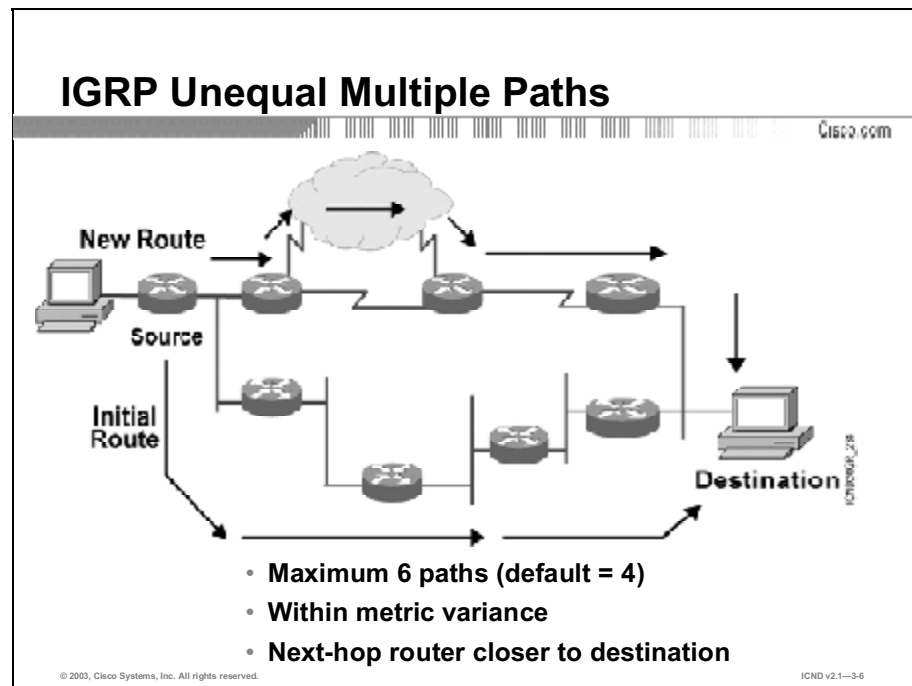
The IGRP metric includes the following components:

- **Bandwidth:** The bandwidth value in the path
- **Delay:** The cumulative interface delay along the path
- **Reliability:** The reliability between source and destination based on keepalives
- **Loading:** The load on a link between source and destination based on bits per second
- **MTU:** The MTU value of the path

By default, only the bandwidth and delay are used by the IGRP metric.

Supporting Multiple Paths with IGRP

The IGRP composite routing metric supports multiple paths between source and destination. This topic describes how multiple paths can be used with IGRP.



The IGRP composite routing metric supports multiple paths between source and destination. Dual equal-bandwidth lines can run a single stream of traffic in a round-robin fashion, with automatic switchover to the second line if one line goes down.

Also, multiple paths can be used, even if the metrics for the paths are different. If, for example, one path is three times better than another path because its metric is three times lower, the better path will be used three times as often. Only routes with metrics that are within a certain range of the best route are used as multiple paths.

Unequal-cost load balancing allows traffic to be distributed among up to six unequal-cost paths to provide greater overall throughput and reliability.

The following general rules apply to IGRP unequal-cost load balancing:

- IGRP will accept up to six (four is the default) paths for a given destination network.
- The next-hop router in any of the paths must be closer to the destination than the local router is by its best path. This ensures that a routing loop will not occur.
- The alternative path metric must be within the specified variance of the best local metric.

Configuring IGRP

Use the **router igrp** and **network** commands to create an IGRP routing process. Use the **variance** and **traffic-share** commands to configure IGRP load balancing. This topic describes how to configure IGRP.

Configuring IGRP



```
Router(config)#router igrp autonomous-system
```

- Defines IGRP as the IP routing protocol

```
Router(config-router)#network network-number
```

- Selects participating attached networks

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—37

Use the **router igrp** and **network** commands to create an IGRP routing process. Note that IGRP requires an autonomous system number. The autonomous system number does not have to be registered. However, all routers within an autonomous system must use the same autonomous system number or they will not exchange routing information.

The **network** command assigns a number to the major network to which the router is directly connected. The IGRP routing process will associate interface addresses with the advertised network number and will begin IGRP packet processing on the specified interfaces.

Configuring IGRP (Cont.)

Cisco.com

```
Router(config-router)#variance multiplier
```

- Controls IGRP load balancing

```
Router(config-router)#traffic-share {balanced | min}
```

- Controls how load-balanced traffic is distributed

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

IGRP supports unequal-cost path load balancing. The **variance** router configuration command controls load balancing in an IGRP environment. Use the **variance *multiplier*** command to configure unequal-cost load balancing by defining the difference between the best metric and the worst acceptable metric, as shown in the table.

variance Command Parameter	Description
<i>multiplier</i>	The range of metric values that will be accepted for load balancing. Acceptable values are nonzero, positive integers. The default value is 1, which means equal-cost load balancing.

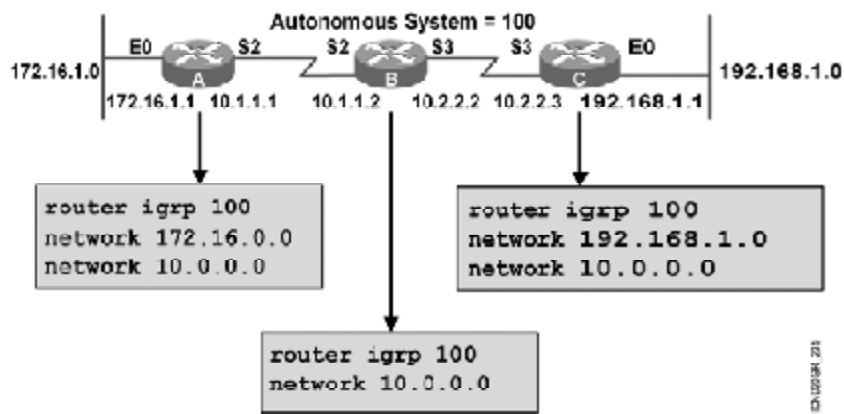
Setting this value lets the router determine the feasibility of a potential route. A route is feasible if the next router in the path is closer to the destination than the current router, and if the metric for the entire path is within the variance. Only paths that are feasible can be used for load balancing and included in the routing table.

You can use the **traffic-share {balanced | min}** command to control how traffic is distributed among IGRP load-sharing routes.

The **traffic-share balanced** command distributes traffic proportionally to the ratios of the metrics. The **traffic-share min** command specifies to use routes that have minimum costs. The default is traffic-shared balanced.

IGRP Configuration Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-9

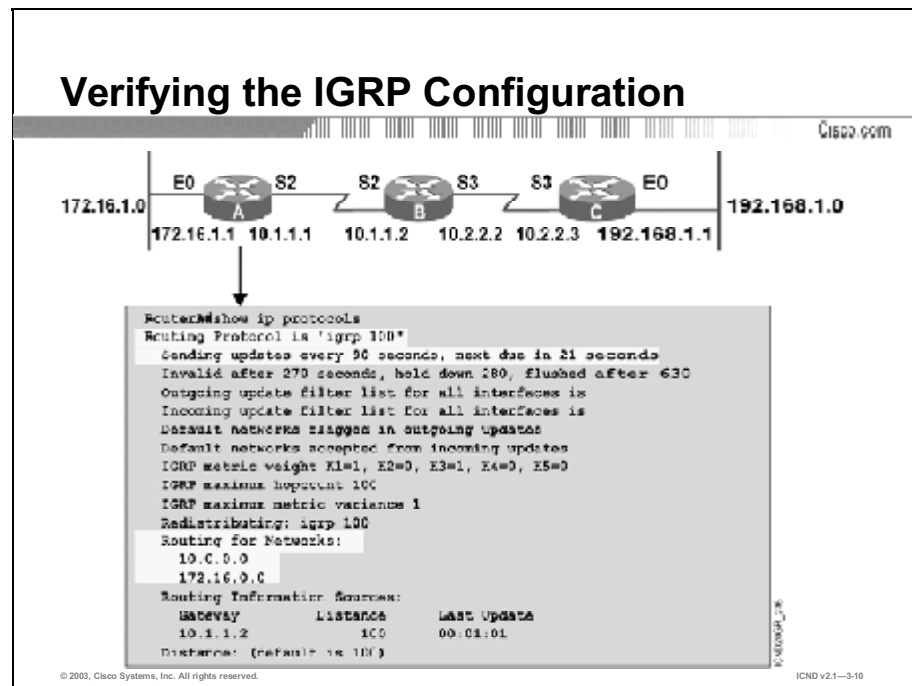
In the example, the following IGRP configurations apply to router A:

Command	Description
router igrp 100	Enables the IGRP routing process for autonomous system 100.
network 172.16.0.0	Associates network 172.16.0.0 with the IGRP routing process.
network 10.0.0.0	Associates network 10.0.0.0 with the IGRP routing process.

IGRP sends updates out of interfaces in the networks 10.0.0.0 and 172.16.0.0, and includes information about the networks 10.0.0.0 and 172.16.0.0, and other networks about which it learns.

Verifying the IGRP Configuration

Use the **show ip protocols** and **show ip route** commands to display information about your IGRP configuration. This topic describes how to verify the IGRP configuration.



Use the **show ip protocols** command to display routing protocol information about the entire router.

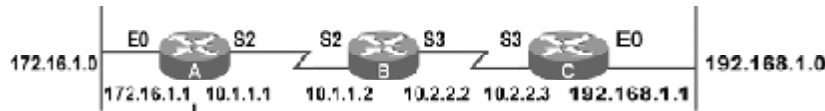
In the figure, the information for IGRP includes the autonomous system, routing timers, networks, and administrative distance.

Output	Description
routing protocol	The routing protocol and autonomous system.
update	Rate at which the periodical routing updates are sent.
invalid	Number of seconds after which a route is declared invalid. The default invalid value should be three times the update value.
holddown	Number of seconds during which routing information regarding the worst path is suppressed. The holddown value should be at least three times the update value.
flush	Number of seconds that must pass before the route is removed from the routing table. The flush value should be equal to or greater than the sum of the invalid and holddown values.

The constants K1, K2, K3, K4, and K5, that are used to weight the metrics in the IGRP routing algorithm, are also displayed with the **show ip protocols** command. Only the bandwidth (K1) and delay (K3) are used in the algorithm by default. These constants are set to 1.

Displaying the IP Routing Table

Cisco.com



```

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

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
I    10.2.2.0 [100/90956] via 10.1.1.2, 00:00:23, Serial2
C    10.1.1.0 is directly connected, Serial2
I    192.168.1.0/24 [100/91055] via 10.1.1.2, 00:00:23, Serial2
  
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-11

Use the **show ip route** command to display the contents of the IP routing table. The table contains a list of all known networks and subnets associated with each entry.

In the figure, the information was learned from IGRP (I) or from direct connections (C). In the routing table, the [100/90956] output is the IGRP administrative distance and the metric.

Troubleshooting the IGRP Configuration

Use the **debug ip igrp transactions** command to display transaction information on IGRP routing transactions and the **debug ip igrp events** command to display a summary of IGRP routing information. This topic describes how to use **debug** commands to troubleshoot an IGRP configuration.

debug ip igrp transaction Command

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on
RouterA#
00:21:06: IGRP: sending update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:21:06:      network 10.0.0.0, metric=88956
00:21:06:      network 192.168.1.0, metric=91056
00:21:07: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:21:07:      network 192.16.0.0, metric=1100
00:21:16: IGRP: received update from 10.1.1.2 on Serial2
00:21:16:      subnet 10.2.2.0, metric 90956 (neighbor 88956)
00:21:16:      network 192.168.1.0, metric 91056 (neighbor 89056)
```

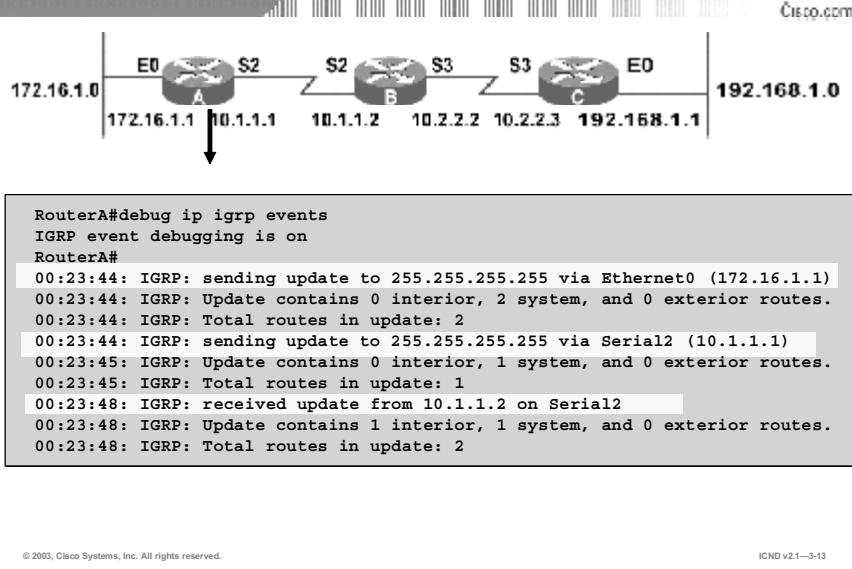
Use the **debug ip igrp transactions** command to display transaction information on IGRP routing transactions. If the IP address of an IGRP neighbor is specified, the resulting output includes only messages describing updates from that neighbor and updates that the router broadcasts toward that neighbor.

debug ip igrp transaction Command Parameter	Description
<i>ip-address</i>	(Optional) IP address of an IGRP neighbor.

The output shows that the router being debugged has also received an update from the router at source address 10.1.1.2, including information about two destinations. The fields are the same as in the sending output, but the metric in parentheses indicates the metric advertised by the neighbor sending the information. “Metric... inaccessible” usually means that the neighbor router has put the destination in holddown.

Use the **no debug ip igrp transaction** or **no debug all** command to disable the debugging output.

debug ip igrp events Command



When there are many networks in your routing table, displaying every update for every route can flood the console and make the router unusable. In this case, use the **debug ip igrp events** command to display a summary of IGRP routing information. The output of this command indicates the source and destination of each update as well as the number of routes in each update. Messages are not generated for each route.

If the IP address of an IGRP neighbor is specified when the **debug ip igrp events** command is issued, the resulting output includes only messages describing updates *from* that neighbor and updates that the router broadcasts *toward* that neighbor. The figure illustrates updates between router A and its neighbors. The table describes the *ip-address* parameter.

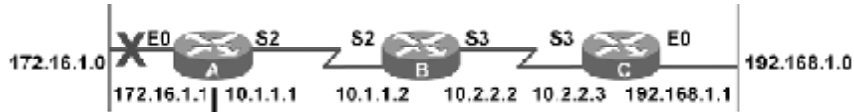
debug ip igrp events Command Parameter	Description
<i>ip-address</i>	(Optional) IP address of an IGRP neighbor.

Use the **no debug ip igrp events** or **no debug all** command to disable the debugging output.

In the figure, router A exchanges update IGRP messages with its neighbors. The router that is being debugged has sent updates, in both cases to the broadcast address 255.255.255.255 as the destination address. In the output line, the first field refers to the type of destination information: “subnet” (interior), “network” (system), or “exterior” (exterior). The second field is the Internet address of the destination network. The third field is the metric stored in the routing table. The numbers in parentheses are the source addresses used in the IP header.

Updating Routing Information Example

Cisco.com



```

ROUTER# debug ip igrp transactions
[0:31:15: %LINKPROTO-S-UPDOWN: Line protocol on Interface E0/Serial0, changed state to down.
[0:31:15: IGRP: addition in net 3
[0:31:15: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
[0:31:15: network 172.16.0.0, metric=4294967295
[0:31:16: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
[0:31:16: IGRP: Total routes in update: 1
[0:31:16: IGRP: broadcasting request on Serial2
[0:31:16: IGRP: received update from 10.1.1.2 on Serial2
[0:31:16: subnet 10.2.2.0, metric 50055 (neighbor 88055)
[0:31:16: network 172.16.0.0, metric 4294967295 (inaccessible)
[0:31:16: network 192.168.1.0, metric 91055 (neighbor 89055)
[0:31:16: IGRP: Update contains 2 interior, 2 system, and 0 exterior routes.
[0:31:16: IGRP: Total routes in update: 3
  
```

© 2003, Cisco Systems, Inc. All rights reserved.

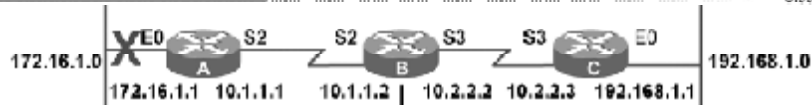
ICND v2.1—3-14

The next few pages describe a routing update scenario using IGRP when an Ethernet connection fails.

In the figure, the Ethernet network attached to router A fails. Router A sends a triggered update to router B indicating that network 172.16.0.0 is inaccessible (with a metric of 4294967295). Router B sends back a poison reverse update.

Updating Routing Information Example (Cont.)

Cisco.com



```
RouterB#debug ip igrp transactions
IGRP protocol debugging is on
RouterB#
1d19h: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.2)
1d19h:   subnet 10.2.2.0, metric=88956
1d19h:   network 192.168.1.0, metric=89055
1d19h: IGRP: sending update to 255.255.255.255 via Serial3 (10.2.2.2)
1d19h:   subnet 10.1.1.0, metric=88956
1d19h:   network 172.16.0.0, metric=89056
1d19h: IGRP: received update from 10.1.1.1 on Serial2
1d19h:   network 172.16.0.0, metric 4294967295 (inaccessible)
1d19h: IGRP: edition is now 10
1d19h: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.2)
1d19h:   subnet 10.2.2.0, metric=88956
1d19h:   network 172.16.0.0, metric=4294967295
1d19h:   network 192.168.1.0, metric=89055
1d19h: IGRP: sending update to 255.255.255.255 via Serial3 (10.2.2.2)
1d19h:   subnet 10.1.1.0, metric=88956
1d19h:   network 172.16.0.0, metric=4294967295
```

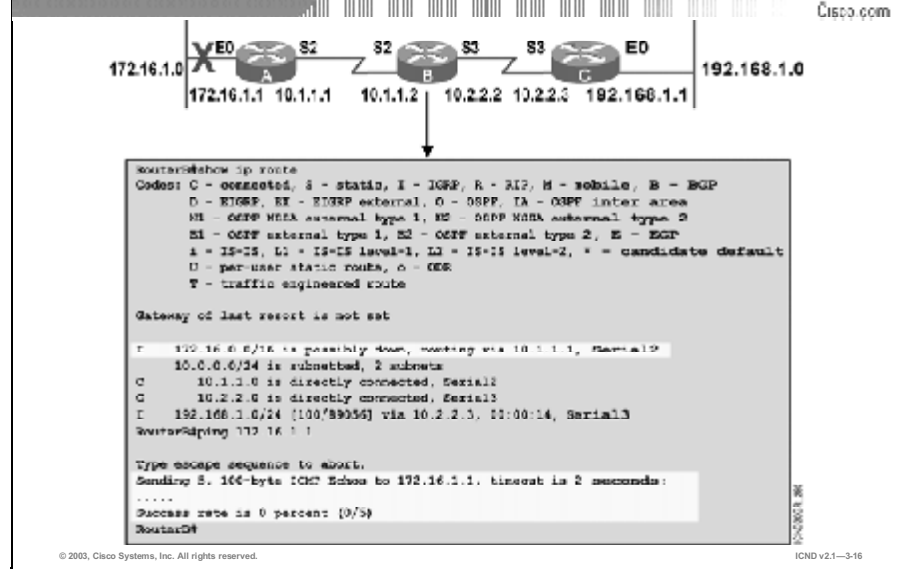
ICND2EN 179

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-15

Router B receives the triggered update from router A, sends a poison reverse to router A, and sends a triggered update to router C, notifying both routers that network 176.16.0.0 is “possibly down.”

Updating Routing Information Example (Cont.)



Router B also places the route to network 172.16.0.0 in the holddown state for 280 seconds. During holddown state, the route to network 172.16.0.0 is marked as “possibly down” in the routing table. Router B will still try to send traffic to network 172.16.0.0 until the holddown timer expires.

In the figure, an administrator attempts to ping network 172.16.0.0 without success.

Updating Routing Information Example (Cont.)

Cisco.com



```
RouterA#show ip eigrp neighbors
RouterA#
LSNbr: LSRP: received update from 10.1.1.1 on Serial3
LSNbr: network 172.16.0.0, metric 89056 (neighbor 1000)
RouterA#
RouterA#sh ip route
Codes: C - connected, S - static, I - IGMP, M - MIB, N - Mobile, B - BGP
D - EIGRP, EX - EIGRP external, L - local, LA - LAMP, IA - LAMP inner area
OA - OSPF external type 1, OE - OSPF external type 2, E - BGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
O - per-link static route, o - OOR
T - traffic engineered route

Gateway of last resort is not set

R
  172.16.0.0/16 is possibly down, routing via 10.1.1.1, Serial32
  10.0.0.0/24 is subnetted, 2 subnets
C    10.1.1.0 is directly connected, Serial32
C    10.2.2.0 is directly connected, Serial33
C    192.168.1.0/24 [120/90056] via 10.2.2.3, 00:10:30, Serial33
RouterA#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.16.0.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/40 ms
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1-3-17

If the link comes back up, router A will send another trigger update to router B stating that network 172.16.0.0 is now accessible (with metric 89056). In the figure, router B receives the triggered update.

Even though router B receives the update, router B will keep the route in holddown state. Router B will not remove the route from holddown state and update its routing table until the holddown timer expires.

In the figure, the holddown timer has not yet expired, so the route is still “possibly down.” However, the administrator at router B can now successfully ping network 172.16.0.0.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- IGRP has several key features such as increased scalability, a sophisticated metric, and multiple paths.
- IGRP uses a composite routing metric that can include bandwidth, delay, reliability, loading, and MTU value.
- The IGRP composite routing metric supports multiple paths between source and destination.
- Use the router igrp and network commands to create an IGRP routing process. Use the variance and traffic-share commands to configure IGRP load balancing.
- Use the show ip protocols and show ip route commands to display information about your IGRP configuration.
- Use the debug ip igrp transaction command to display transaction information on IGRP routing transactions and the debug ip igrp events command to display a summary of the IGRP routing information.

© 2003, Cisco Systems, Inc. All rights reserved. IGRND v2.1—3-18

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you have learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which two factors can be included in an IGRP composite routing metric? (Choose two.)
- A) cost
 - B) delay
 - C) hop count
 - D) bandwidth
 - E) cable distance
- Q2) IGRP has a default maximum hop count of _____ hops, configurable to a maximum of _____ hops.
- A) 6; 15
 - B) 15; 100
 - C) 100; 255
 - D) 200; 255
- Q3) Which two components are used by default in the IGRP composite metric? (Choose two.)
- A) delay
 - B) loading
 - C) reliability
 - D) bandwidth
 - E) MTU value
- Q4) With IGRP, the best path is the one that has which characteristic?
- A) the lowest hop count
 - B) the highest hop count
 - C) the lowest metric value
 - D) the highest metric value

- Q5) With IGRP unequal-cost load balancing, which two conditions must be met for each of the paths? (Choose two.)
- A) The metric must be equal to the best path metric.
 - B) The metric must be within a specified variance of the best path metric.
 - C) The next-hop router must be closer to the destination than the local router is by its best path.
 - D) The next-hop router must be farther from the destination than the local router is by its best path.
- Q6) Up to _____ multiple paths can be defined for a given destination, with _____ being the default maximum.
- A) 8; 6
 - B) 6; 4
 - C) 6; 6
 - D) 8; 8
- Q7) Which command will distribute traffic across IGRP multiple paths proportionally to the ratios of the metrics?
- A) **variance 1**
 - B) **traffic-share min**
 - C) **traffic-share balanced**
 - D) **traffic-share variance 1**
- Q8) What is the result of the **variance 2** command in an IGRP configuration?
- A) The metric of a feasible alternate path to a destination can be a value no more than the best path metric to that destination plus 2.
 - B) The metric of a feasible alternate path to a destination can be a value no less than the best path metric to that destination minus 2.
 - C) The metric of a feasible alternate path to a destination can be no more than 1/2 of the metric of the best path metric to that destination.
 - D) The metric of a feasible alternate path to a destination can be no more than two times the metric of the best path metric to that destination.
- Q9) In the output of the **show ip protocols** command, what is specified by “flushed after 630”?
- A) An update to a route that was invalid and is now up will not be made until 630 seconds have passed.
 - B) The router will wait 630 seconds before requesting an update from a router that is no longer sending updates.
 - C) If the router does not receive an update from another router for 630 seconds or more, it marks the routes served by that other router as being invalid.
 - D) If the router does not receive an update from another router for 630 seconds or more, the router removes all routing table entries learned from that other router.

- Q10) Which command displays a summary of IGRP routing activity?
- A) **debug ip igrp events**
 - B) **debug ip igrp transactions**
 - C) **debug ip igrp events summary**
 - D) **debug ip igrp transactions summary**
- Q11) In the output of the **debug ip igrp transactions** command, what does “(neighbor 88765)” indicate?
- A) the MAC address of the neighbor sending the update
 - B) the number of times that neighbor has advertised the route
 - C) the metric for reaching the neighbor from the current router
 - D) the metric advertised by the neighbor sending the information

Quiz Answer Key

- Q1) B, D
Relates to: IGRP Features
- Q2) C
Relates to: IGRP Features
- Q3) A, D
Relates to: IGRP Metrics
- Q4) C
Relates to: IGRP Metrics
- Q5) B, C
Relates to: Supporting Multiple Paths with IGRP
- Q6) B
Relates to: Supporting Multiple Paths with IGRP
- Q7) C
Relates to: Configuring IGRP
- Q8) D
Relates to: Configuring IGRP
- Q9) D
Relates to: Verifying the IGRP Configuration
- Q10) A
Relates to: Troubleshooting the IGRP Configuration
- Q11) D
Relates to: Troubleshooting the IGRP Configuration

Enabling EIGRP

Overview

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the IGRP developed by Cisco Systems. EIGRP is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal overhead. This lesson describes how to configure and monitor EIGRP.

Relevance

EIGRP is a popular choice for routing protocol on Cisco devices. As such, you should know how to configure EIGRP.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of EIGRP
- Use Cisco IOS commands to configure dynamic routing using EIGRP, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using EIGRP, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

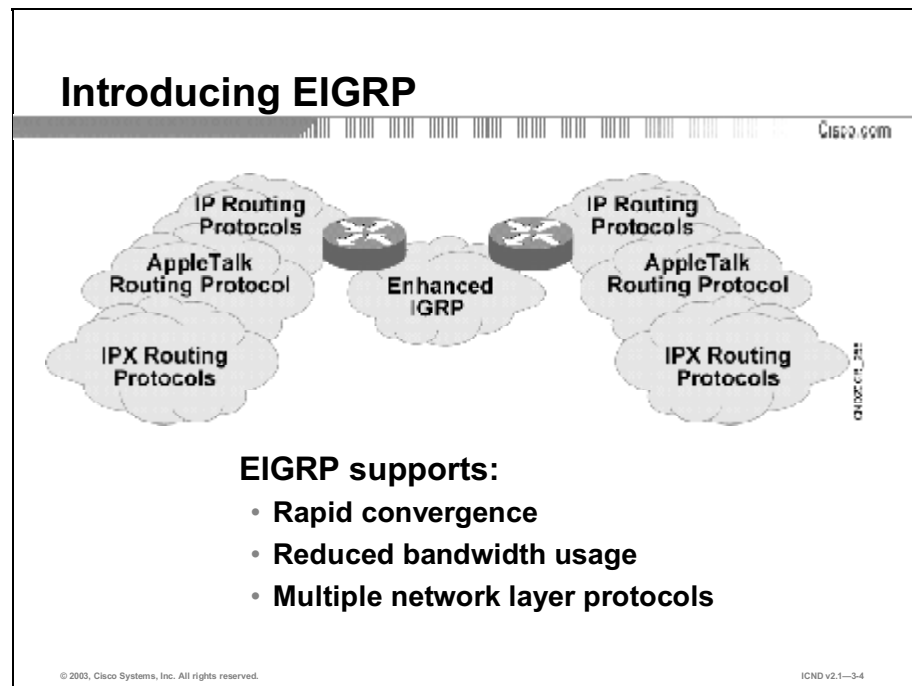
Outline

The lesson includes these topics:

- Overview
- EIGRP Features
- Comparing EIGRP and IGRP
- Configuring EIGRP Protocol
- Verifying the EIGRP Configuration
- Troubleshooting the EIGRP Configuration
- Summary
- Quiz

EIGRP Features

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol suited for many different topologies and media. This topic describes the features of EIGRP.

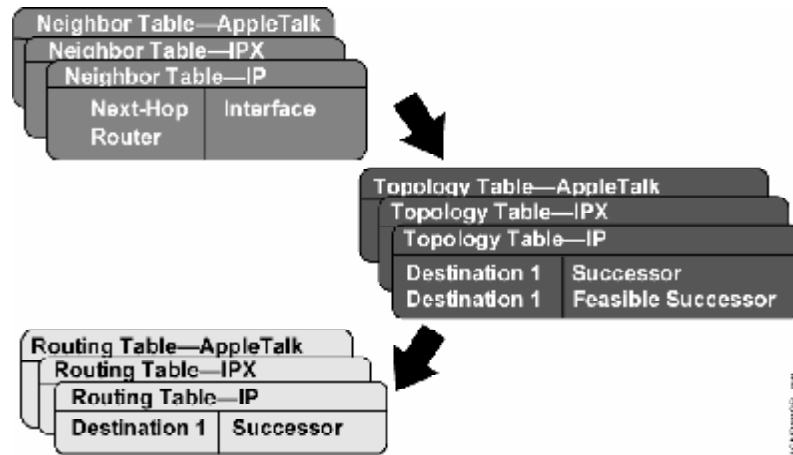


In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. Some of the many advantages of EIGRP are:

- Rapid convergence times for changes in the network topology. In some situations convergence can be almost instantaneous. EIGRP uses the Diffusing Update Algorithm (DUAL) to achieve rapid convergence. A router running EIGRP stores backup routes for destinations, when available, so it can quickly adapt to alternate routes. If no appropriate route or backup route exists in the local routing table, EIGRP queries its neighbors to discover an alternate route. These queries are propagated until an alternate route is found.
- Very low usage of network resources during normal operation; only “hello” packets are transmitted on a stable network. Like other link-state routing protocols, EIGRP uses EIGRP hello packets to establish neighbor relationships with other EIGRP neighboring routers. Each router builds a neighbor table from the hello packets that it receives from adjacent EIGRP routers. EIGRP does *not* send periodic routing updates like Interior Gateway Routing Protocol (IGRP). When a change occurs, only routing table changes are propagated, not the entire routing table: this reduces the load that the routing protocol itself places on the network by minimizing the bandwidth that is required for EIGRP packets.
- EIGRP supports automatic (classful) route summarization at major network boundaries as the default. However, unlike other classful routing protocols like IGRP and Routing Information Protocol (RIP), manual route summarization can be configured on arbitrary network boundaries to reduce the size of the routing table.

EIGRP Terminology

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

The table summarizes several terms related to EIGRP.

Term	Definition
Neighbor table (AppleTalk, IPX ¹ , IP)	Each EIGRP router maintains a neighbor table that lists adjacent routers. This table is comparable to the adjacencies database used by OSPF ² . It serves the same purpose: to ensure bidirectional communication between each of the directly connected neighbors. There is a neighbor table for each protocol that EIGRP supports.
Topology table (AppleTalk, IPX, IP)	Each EIGRP router maintains a topology table for each configured routing protocol. This table includes route entries for all destinations that the router has learned. All learned routes to a destination are maintained in the topology table.
Routing table (AppleTalk, IPX, IP)	EIGRP chooses the best (successor) routes to a destination from the topology table and places these routes in the routing table. The router maintains one routing table for each network protocol.
Successor	A route selected as the primary route that is used to reach a destination. Successors are the entries kept in the routing table.
Feasible successor	A backup route. These routes are selected at the same time the successors are identified, but they are kept in a topology table. Multiple feasible successors for a destination can be retained.

¹IPX = Internetwork Packet Exchange

²OSPF = Open Shortest Path First

Comparing EIGRP and IGRP

EIGRP is an enhanced version of the IGRP developed by Cisco Systems, with improved convergence properties and operating efficiency over IGRP. This topic compares EIGRP to IGRP.

Comparing EIGRP and IGRP

Cisco.com

- **Similar metric**
- **Same load balancing**
- **Improved convergence time**
- **Reduced network overhead**

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—3-6

EIGRP uses similar metric calculations and supports unequal cost path load balancing like IGRP. However, the convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP. While the metric (bandwidth and delay by default) is the same for both IGRP and EIGRP, the weight assigned to the metric is 255 times greater for EIGRP.

The convergence technology is based on the research conducted at SRI International and employs DUAL. This algorithm guarantees loop-free operation at every instant throughout a route computation, and allows all devices involved in a topology change to synchronize at the same time. Routers that are *not* affected by topology changes are not involved in recomputations. The convergence time with DUAL rivals that of any other existing routing protocol.

Configuring EIGRP Protocol

Use the **router eigrp** and **network** commands to create an EIGRP routing process. This topic describes how to configure EIGRP.

Configuring EIGRP



```
Router(config)#router eigrp autonomous-system
```

- Defines EIGRP as the IP routing protocol

```
Router(config-router)#network network-number
```

- Selects participating attached networks

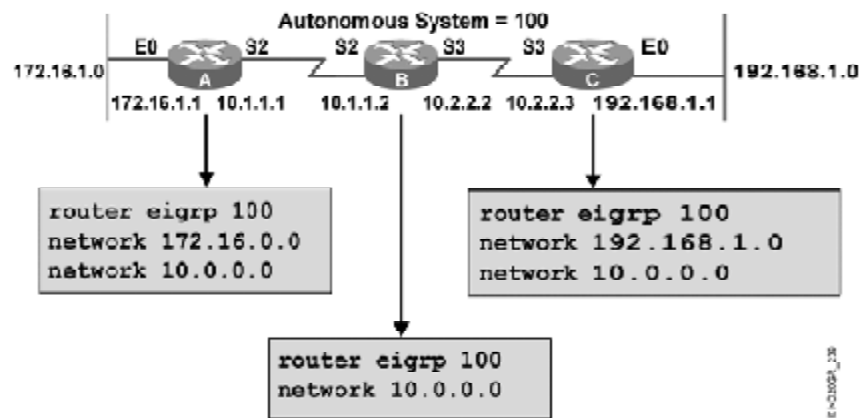
© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-7

Use the **router eigrp** and **network** commands to create an EIGRP routing process. Note that EIGRP requires an autonomous system number. The autonomous system number does not have to be registered. However, all routers within an autonomous system must use the same autonomous system number or they will not exchange routing information.

The **network** command assigns a major network number to which the router is directly connected. The EIGRP routing process will associate interface addresses with the advertised network number and will begin EIGRP packet processing on the specified interfaces.

EIGRP Configuration Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

In the EIGRP configuration example, the following table applies to EIGRP configurations on router A:

Command	Description
<code>router eigrp 100</code>	Enables the EIGRP routing process for autonomous system 100.
<code>network 172.16.0.0</code>	Associates network 172.16.0.0 with the EIGRP routing process.
<code>network 10.0.0.0</code>	Associates network 10.0.0.0 with the EIGRP routing process.

EIGRP sends updates out of the interfaces in networks 10.0.0.0 and 172.16.0.0, and includes information about networks 10.0.0.0 and 172.16.0.0, as well as other networks about which it learns.

Verifying the EIGRP Configuration

Use the **show ip eigrp** commands to display information about the EIGRP configuration. This topic describes how to verify the EIGRP configuration.

Verifying the EIGRP Configuration

Router#show ip eigrp neighbors

- Displays the neighbors discovered by IP EIGRP

Router#show ip eigrp topology

- Displays the IP EIGRP topology table

Router#show ip route eigrp

- Displays current EIGRP entries in the routing table

Router#show ip protocols

- Displays the parameters and current state of the active routing protocol process

Router#show ip eigrp traffic

- Displays the number of IP EIGRP packets sent and received

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-9

Use the following **show** commands to verify EIGRP operation:

Command	Description
show ip eigrp neighbors	Displays neighbors discovered by EIGRP.
show ip eigrp topology	Displays the EIGRP topology table. This command shows the topology table, the active or passive state of routes, the number of successors, and the feasible distance to the destination.
show ip route eigrp	Displays the current EIGRP entries in the routing table.
show ip protocols	Displays the parameters and current state of the active routing protocol process. This command shows the EIGRP autonomous system number. It also displays filtering and redistribution numbers, as well as neighbors and distance information.
show ip eigrp traffic	Displays the number of EIGRP packets sent and received. This command displays statistics on hello, updates, queries, replies, and acknowledgments.

Troubleshooting the EIGRP Configuration

To display information on EIGRP protocol packets, use the **debug ip eigrp** privileged EXEC command. This topic describes the **debug** command to troubleshoot an EIGRP configuration.

debug ip eigrp Command



```
Router#debug ip eigrp
IP-EIGRP: Processing incoming UPDATE packet
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.246.0 255.255.255.0 metric 46310656 - 45714176 596480
IP-EIGRP: 172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP: 192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP: 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-10

This command helps you analyze the packets that are sent and received on an interface. Because the **debug ip eigrp** command generates a substantial amount of output, use it only when traffic on the network is light.

The table describes the fields in the sample output from the **debug ip eigrp** command:

Field	Description
IP-EIGRP:	Indicates that this is an IP EIGRP packet.
Ext	Indicates that the following address is an external destination rather than an internal destination, which would be labeled as Int.
M	Displays the computed metric, which includes SM and the cost between this router and the neighbor. The first number is the composite metric. The next two numbers are the inverse bandwidth and the delay, respectively.
SM	Displays the metric as reported by the neighbor.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **EIGRP is an interior gateway protocol suited for many different topologies and media.**
- **EIGRP is an enhanced version of the IGRP developed by Cisco, with improved convergence properties and operating efficiency over IGRP.**
- **Use the router eigrp and network commands to create an EIGRP routing process.**
- **Use the show ip eigrp commands to display information about the EIGRP configuration.**
- **To display information on EIGRP packets, use the debug ip eigrp privileged EXEC command.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-11

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) With EIGRP, how can propagating only routing table changes rather than the entire routing table improve network performance?
- A) by minimizing the scalability requirements
 - B) by minimizing the time required to achieve convergence
 - C) by minimizing the amount of bandwidth required for hello packets
 - D) by minimizing the amount of bandwidth required for EIGRP packets
- Q2) EIGRP chooses the best (successor) routes to a destination from the _____ and places these routes in the _____.
- A) topology table, routing table
 - B) routing table, neighbor table
 - C) neighbor table, routing table
 - D) topology table, neighbor table
- Q3) Which two features are the same in both EIGRP and IGRP? (Choose two.)
- A) composite metric
 - B) hop count metric
 - C) convergence time
 - D) network overhead
 - E) unequal-cost load balancing
- Q4) What are two features of the DUAL algorithm in EIGRP? (Choose two.)
- A) guaranteed loop-free operation
 - B) involves all routers in route recomputations
 - C) convergence time in the top ten of all existing protocols
 - D) convergence time rivaling that of any other available protocol
 - E) allows all devices involved in a topology change to synchronize within seconds of each other
- Q5) Which command correctly enables an EIGRP routing process and assigns the router to autonomous system 200?
- A) Router(config)#**network 200**
 - B) Router(config)#**router eigrp 200**
 - C) Router(config-router)#**network 200**
 - D) Router(config-router)#**router eigrp AS 200**

- Q6) Which command displays the EIGRP cost to a specific destination?
- A) **show ip eigrp traffic**
 - B) **show ip eigrp topology**
 - C) **show ip eigrp interfaces**
 - D) **show ip eigrp neighbors**
- Q7) In the output of the **show ip eigrp neighbors** command, what is indicated by the number in “process 77”?
- A) major network number
 - B) autonomous system number
 - C) number of EIGRP processes running
 - D) number of routes learned through EIGRP
- Q8) In the output of the **debug ip eigrp** command, what is specified by the 256000 in “M 386560 – 256000 130560”?
- A) delay
 - B) computed metric
 - C) inverse bandwidth
 - D) metric advertised by the neighbor
- Q9) Which label specifies the metric as advertised by the neighbor in the output of the **debug ip eigrp** command?
- A) M
 - B) SM
 - C) Int
 - D) Ext

Quiz Answer Key

- Q1) D
Relates to: EIGRP Features
- Q2) A
Relates to: EIGRP Features
- Q3) A, E
Relates to: Comparing EIGRP and IGRP
- Q4) A, D
Relates to: Comparing EIGRP and IGRP
- Q5) B
Relates to: Configuring EIGRP Protocol
- Q6) B
Relates to: Verifying the EIGRP Configuration
- Q7) B
Relates to: Verifying the EIGRP Configuration
- Q8) C
Relates to: Troubleshooting the EIGRP Configuration
- Q9) B
Relates to: Troubleshooting the EIGRP Configuration

Enabling OSPF

Overview

Open Shortest Path First (OSPF) is an interior gateway protocol. Unlike Interior Gateway Routing Protocol (IGRP), OSPF is a classless link-state routing protocol rather than a classful distance vector protocol. This lesson describes the function of OSPF and how to configure a single area OSPF network on a Cisco Systems router.

Relevance

Because OSPF is widely deployed, knowledge of its configuration and maintenance is essential.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of the OSPF protocol
- Use Cisco IOS commands to configure dynamic routing for a single area OSPF network, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using OSPF, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

Outline

The lesson includes these topics:

- Overview
- OSPF Features
- Comparing OSPF with Distance Vector Routing Protocols
- Shortest Path Algorithm
- Configuring Single Area OSPF
- Verifying the OSPF Configuration
- Troubleshooting the OSPF Configuration
- Summary
- Quiz

OSPF Features

Open Shortest Path First (OSPF) is an interior gateway protocol similar to Interior Gateway Routing Protocol (IGRP), but based on link states rather than distance vectors. This topic describes the features of OSPF.

Introducing OSPF



The diagram shows a cloud-like shape representing a network. Inside the cloud, there are several circular icons representing routers, each with a cross symbol. The word "OSPF" is written in the center of the cloud. To the right of the cloud, there is a vertical text label "OSPF".

- **Open standard**
- **Shortest path first (SPF) algorithm**
- **Link-state routing protocol (vs. distance vector)**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-4

OSPF is a routing protocol developed for IP networks by the Interior Gateway Protocol (IGP) working group of the Internet Engineering Task Force (IETF). The working group was formed in 1988 to design an IGP based on the shortest path first (SPF) algorithm. Similar to the IGRP, OSPF was created because in the mid-1980s, the Routing Information Protocol (RIP) was increasingly incapable of serving large, heterogeneous internetworks. OSPF routes packets within a single autonomous system. The OSPF protocol is based on link-state technology, as opposed to distance vector based algorithms that are used in traditional Internet intra-domain routing protocols such as RIP.

OSPF has two primary characteristics. The first is that the protocol is an open standard, which means that its specification is in the public domain. The OSPF specification is published as RFC. The IETF developed OSPF in 1988. The most recent version, known as OSPF version 2, is described in RFC 2328.

The second principal characteristic is that OSPF is based on the SPF algorithm, which sometimes is referred to as Dijkstra's algorithm, named for the person credited with its creation.

Comparing OSPF with Distance Vector Routing Protocols

OSPF advertises information about each of its links rather than sending periodic routing table updates like a distance vector protocol. This topic compares OSPF routing with distance vector routing.

OSPF as a Link-State Protocol

Cisco.com

- **OSPF propagates link-state advertisements rather than routing table updates.**
- **LSAs are flooded to all OSPF routers in the area.**
- **The OSPF link-state database is pieced together from the LSAs generated by the OSPF routers.**
- **OSPF uses the SPF algorithm to calculate the shortest path to a destination.**
 - **Link = router interface**
 - **State = description of an interface and its relationship to neighboring routers**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

OSPF is a link-state protocol. You can think of a *link* as being an interface on a router. The state of the link is a description of that interface and of its relationship to its neighboring routers. A description of the interface would include, for example, the IP address of the interface, the mask, the type of network to which it is connected, the routers connected to that network, and so on. The collection of all these link states forms a *link-state database*.

OSPF calls for the sending of link-state advertisements (LSAs) to all other routers within the same hierarchical area. A router sends LSA packets to advertise its state periodically (at long intervals, such as every 30 minutes) and when the router state changes. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node.

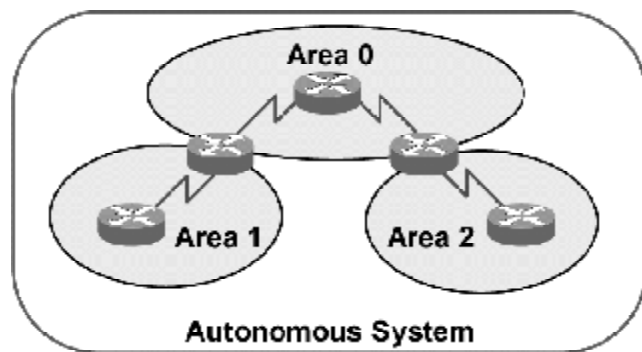
As a link-state routing protocol, OSPF contrasts with RIP and IGRP, which are distance vector routing protocols. Routers running the distance vector algorithm send all or a portion of their routing tables in routing-update messages to their neighbors.

Unlike RIP, IGRP, and EIGRP, OSPF can operate within a hierarchy. The largest entity within the hierarchy is the autonomous system, which is a collection of networks under a common administration that share a common routing strategy. An autonomous system can be divided into a number of areas, which are groups of contiguous networks and attached hosts.

A topological (link-state) database is essentially an overall picture of networks in relationship to routers. The topological database contains the collection of LSAs received from all routers in the same area. Because routers within the same area share the same information, they have identical topological databases.

OSPF Hierarchical Routing

Cisco.com



- **Consists of areas and autonomous systems**
- **Minimizes routing update traffic**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-6

The OSPF ability to separate a large internetwork into multiple areas is also referred to as hierarchical routing. Hierarchical routing enables you to separate a large internetwork (autonomous system) into smaller internetworks that are called areas.

With this technique, routing still occurs between the areas (called interarea routing), but many of the minute internal routing operations, such as recalculating the database, are kept within an area.

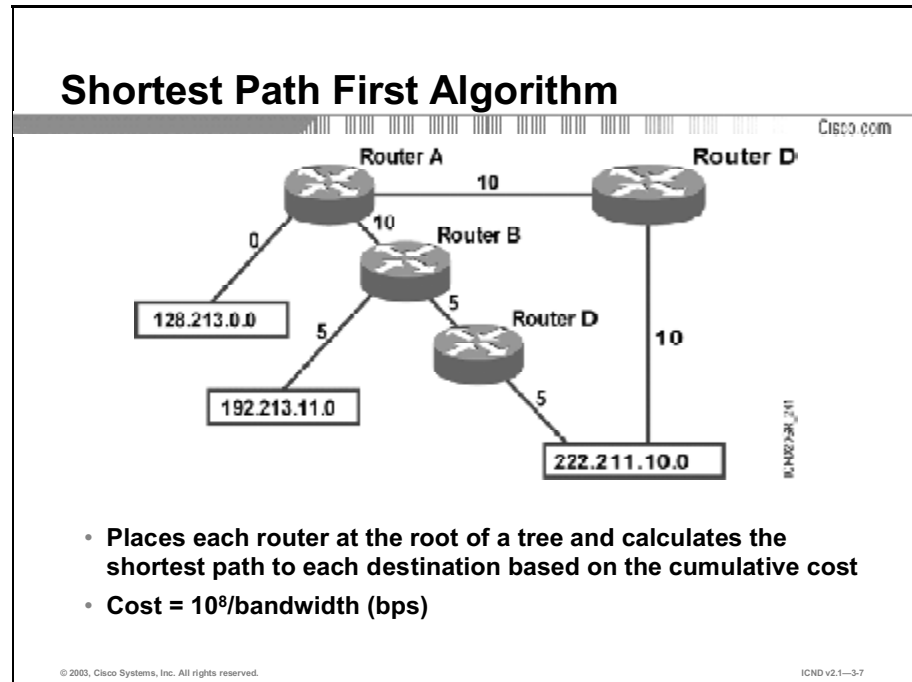
For example, in the figure, if Area 1 is having problems with a link going up and down, routers in other areas need not continually run their SPF calculation because they are isolated from the Area 1 problem.

The hierarchical topology possibilities of OSPF have some important advantages:

- Reduced frequency of SPF calculations
- Smaller routing tables
- Reduced link-state update overhead

Shortest Path Algorithm

The SPF algorithm places each router at the root of a tree and calculates the shortest path to each node based on the cumulative cost required to reach that destination. This topic describes the SPF algorithm.



LSAs are flooded throughout the area using a reliable algorithm, which ensures that all routers in an area have exactly the same topological database. Each router uses the information in its topological database to calculate a shortest-path tree, with itself as the root. The router then uses this tree to route network traffic. In the figure, router A is the root.

The shortest path is calculated using Dijkstra's algorithm. The algorithm places each router at the root of a tree and calculates the shortest path to each destination based on the cumulative cost required to reach that destination. Each router will have its own view of the topology, even though all the routers will build a shortest-path tree using the same link-state database.

The cost, or metric, of an interface is an indication of the overhead that is required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface, so a higher bandwidth indicates a lower cost. There is more overhead, higher cost, and more time delays involved in crossing a 56 kbps serial line than crossing a 10 Mbps Ethernet line.

The default formula used to calculate OSPF cost is:

$$\text{cost} = 100000000 / \text{bandwidth in bps}$$

For example, it will cost $10^8/10^7 = 10$ to cross a 10M Ethernet line and will cost $10^8/1544000 = 64$ to cross a T1 line.

Configuring Single Area OSPF

Use the **router ospf** command to start an OSPF routing process and the **network** command to associate addresses to an OSPF area. This topic describes how to configure OSPF with a single area.

Configuring Single Area OSPF

Cisco.com

```
Router(config)#router ospf process-id
```

- Defines OSPF as the IP routing protocol

```
Router(config-router)#network address mask area area-id
```

- Assigns networks to a specific OSPF area

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

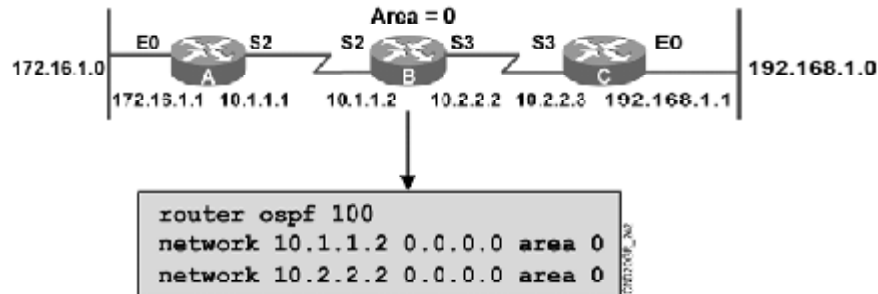
The **router ospf** command takes a process identifier as an argument. This is a unique, arbitrary number that you select to identify the routing process. The process-ID does not need to match the OSPF process-ID on other OSPF routers.

The **network** command identifies which IP networks on the router that are part of the OSPF network. For each network, you must also identify the OSPF area to which the networks belong. The **network** command takes three arguments:

router ospf Command Parameters	Description
<i>address</i>	Can be the network, subnet, or the interface address.
<i>wildcard-mask</i>	Wildcard mask. This masks identifies the part of the IP address to be matched, where “0” is a match and a “1” is do not care. For example, a wildcard mask of 0.0.0.0 indicates a match of all 32 bits in the address.
<i>area-id</i>	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or in dotted-decimal notation.

OSPF Configuration Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-9

In this example, router B has specified 191 as the local process ID for the OSPF routing process. Addresses that begin with 10 as the first octet are assigned to area 0 (the backbone area). In this case, both the S2 and S3 interface on router B will be in OSPF area 0. Both routers A and C will have similar configurations specifying addresses in area 0.

Routers that share a common segment become neighbors on that segment. In the diagram, routers A and C are neighbors of router B, but not of each other.

A router uses the OSPF hello protocol to establish neighbor relationships. Hello packets also act as keepalives to let routers know that other routers are still functional.

On multiaccess networks (networks supporting more than two routers) such as Ethernet networks, the hello protocol elects a designated router (DR) and a backup designated router (BDR). Among other things, the designated router is responsible for generating LSAs for the entire multiaccess network. Designated routers allow a reduction in routing update traffic and manage link-state synchronization. The DR and BDR are elected based on the OSPF priority and OSPF router ID. In non-multiaccess networks like a point-to-point serial link, there will not be a DR or BDR elected.

Calculating wildcard masks on non-8-bit boundaries can be error-prone. Therefore, a method to overcome this is to have a network statement that matches the IP address on each interface.

Configuring Loopback Interfaces

Cisco.com

Unadvertised Loopback Address

Ex: 192.168.255.254

- Not in OSPF table
- Saves address space
- Cannot use ping

Advertised Loopback Address

Ex: 172.16.17.5

- In OSPF table
- Uses address space
- Can use ping



ICND 000R_088

Router ID:

- Number by which the router is known to OSPF
- Default: The highest IP address on an active interface at the moment of OSPF process startup
- Can be overridden by a loopback interface: Highest IP address of any active loopback interface

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-10

To modify the OSPF router ID to a loopback address, first define a loopback interface:

```
Router(config)#interface loopback number
```

The highest IP address used as the router ID can be overridden by configuring an IP address on a loopback interface. OSPF is more reliable if a loopback interface is configured because the interface is always active and cannot go down like a real interface. For this reason it is recommended that you use the loopback address on all key routers. If you plan to publish your loopback address with the **network area** command, you may consider using a private IP address to save on your registered IP address space. Note that a loopback address requires a different subnet for each router, unless the host address itself is advertised.

There are pros and cons to using an address that will not be advertised versus using an address that will be advertised. Using an unadvertised address saves on real IP address space, but the address does not appear in the OSPF table and therefore cannot be pinged. This choice represents a trade-off between the ease of debugging the network and conservation of address space.

Verifying the OSPF Configuration

You can use any one of a number of **show** commands to display information about an OSPF configuration. This topic describes how to verify an OSPF configuration using a few of the **show** commands.

Verifying the OSPF Configuration



Router#show ip protocols

- Verifies that OSPF is configured

Router#show ip route

- Displays all the routes learned by the router

Router#show ip ospf interface

- Displays area-ID and adjacency information

Router#show ip ospf neighbor

- Displays OSPF neighbor information on a per-interface basis

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-11

The **show ip protocols** command displays parameters about timers, filters, metrics, networks, and other information for the entire router.

The **show ip route** command displays the routes known to the router and how they were learned. This command is one of the best ways to determine connectivity between the local router and the rest of the internetwork.

The **show ip ospf interface** command verifies that interfaces have been configured in the intended areas. If no loopback address is specified, the interface with the highest address is chosen as the router ID. This command also displays the timer intervals, including the hello interval, and shows the neighbor adjacencies.

The **show ip ospf neighbor** command displays OSPF neighbor information on a per-interface basis.

Troubleshooting the OSPF Configuration

To display information on OSPF-related events, such as adjacencies, flooding information, designated router selection, and SPF calculation, use the **debug ip ospf events** privileged EXEC command. This topic describes the **debug** commands used to troubleshoot an OSPF configuration.

OSPF debug commands



```
Router#debug ip ospf events

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
Router# debug ip ospf packet

OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.117
      aid:0.0.0.0 chk:6AB2 aut:0 auk:

Router#debug ip ospf packet

OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.116
      aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0
```

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-12

The **debug ip ospf events** output shown might appear if any of the following situations occur:

- The IP subnet masks for routers on the same network do not match.
- The OSPF hello interval for the router does not match that configured for a neighbor.
- The OSPF dead interval for the router does not match that configured for a neighbor.

If a router configured for OSPF routing is not seeing an OSPF neighbor on an attached network, perform the following tasks:

- Make sure that both routers have been configured with the same IP mask, OSPF hello interval, and OSPF dead interval.
- Make sure that both neighbors are part of the same area type.

In the following example line, the neighbor and this router are not both part of a stub area (that is, one is a part of a transit area and the other is a part of a stub area, as explained in RFC 1247):

```
OSPF: hello packet with mismatched E bit
```

To display information about each OSPF packet received, use the **debug ip ospf packet** privileged EXEC command. The **no** form of this command disables debugging output.

The **debug ip ospf packet** command produces one set of information for each packet received. The output varies slightly depending on which authentication is used. The following is sample

output from the **debug ip ospf packet** command when Message Digest 5 (MD5) authentication is used.

The table describes the fields shown in the **debug ip ospf packet** display.

Field	Description
v :	OSPF version
t :	OSPF packet type. Possible packet types are: 1: Hello 2: Data description 3: Link state request 4: Link state update 5: Link state acknowledgment
l :	OSPF packet length in bytes
rid:	OSPF router ID
aid:	OSPF area ID
chk:	OSPF checksum
aut :	OSPF authentication type. Possible authentication types are: 0: No authentication 1: Simple password 2: MD5
auk :	OSPF authentication key
keyid:	MD5 key ID
seq:	Sequence number

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **OSPF is an interior gateway protocol similar to IGRP, but based on link states rather than distance vectors.**
- **OSPF advertises information about each of its links rather than sending routing table updates like a distance vector protocol.**
- **The SPF algorithm places each router at the root of a tree and calculates the shortest path to each destination based on the cumulative cost required to reach that destination.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-13

Summary (Cont.)

Cisco.com

- **Use the router ospf command to start an OSPF routing process and the network command to associate addresses to an OSPF area.**
- **You can use any one of a number of show commands to display information about an OSPF configuration.**
- **To display information on OSPF-related events, such as adjacencies, flooding information, designated router selection, and SPF calculation, use the debug ip ospf events privileged EXEC command.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-14

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What are two characteristics of OSPF? (Choose two.)
- A) open standard
 - B) link-state protocol
 - C) distance vector protocol
 - D) classful routing protocol like RIP and IGRP
 - E) support multiple routed protocols, including IP, Internetwork Packet Exchange (IPX), and AppleTalk
- Q2) In OSPF, what term specifies a description of an interface and of its relationship to its neighboring routers?
- A) link state
 - B) distance vector
 - C) link-state database
 - D) link-state advertisement
- Q3) What is an OSPF link?
- A) a cable
 - B) a network
 - C) an interface
 - D) a network segment
- Q4) With the shortest path first algorithm, the shortest path to a node is determined by calculating ____.
- A) the number of hops
 - B) the cumulative cost of crossing each link
 - C) the cumulative cost of network equipment
 - D) the cumulative cost of traversing each network segment
- Q5) What is the default formula to calculate link cost in the SPF algorithm?
- A) $10^8/\text{bandwidth in bps}$
 - B) $\text{bandwidth in bps}/10^8$
 - C) $10^8/\text{bandwidth in kbps}$
 - D) $\text{bandwidth in kbps}/10^8$

- Q6) Which command correctly assigns addresses beginning with 198.172 to OSPF area 0?
- A) **Router(config)#router ospf 198.172.0.0 0.0.255.255 area 0**
 - B) **Router(config)#router ospf 198.172.0.0 255.255.0.0 area 0**
 - C) **Router(config-router)#network 198.172.0.0 0.0.255.255 area 0**
 - D) **Router(config-router)#network 198.172.0.0 255.255.0.0 area 0**
- Q7) Which command defines a loopback interface so you can modify the OSPF router ID to a loopback address?
- A) Router(config)#**router ospf loopback**
 - B) Router(config)#**router ip ospf loopback**
 - C) Router(config)#**interface number loopback**
 - D) Router(config)#**interface loopback number**
- Q8) What is the purpose of the **show ip ospf interface** command?
- A) to display OSPF-related interface information
 - B) to display OSPF neighbor information on a per-interface basis
 - C) to verify that interfaces have been configured in the intended areas
 - D) to display OSPF neighbor information on a per-interface type basis
- Q9) Which Cisco IOS command displays the routes known to the router and how they were learned?
- A) **show ip ospf**
 - B) **show ip route**
 - C) **show ip protocols**
 - D) **show ip ospf interface**
- Q10) If the output of the **debug ip ospf events** command includes “OSPF: hello with invalid timers,” what might have caused the error?
- A) The hello intervals on the two routers do not match.
 - B) The area routers for the two networks do not match.
 - C) The metrics advertised by the two routers do not match.
 - D) The autonomous system numbers for the two routers do not match.
- Q11) Which number in the OSPF packet type field of the output from the **debug ip ospf packet** command indicates a link-state update?
- A) 1
 - B) 2
 - C) 3
 - D) 4

Quiz Answer Key

- Q1) A, B
Relates to: OSPF Features
- Q2) A
Relates to: Comparing OSPF with Distance Vector Routing Protocols
- Q3) C
Relates to: Comparing OSPF with Distance Vector Routing Protocols
- Q4) B
Relates to: Shortest Path Algorithm
- Q5) A
Relates to: Shortest Path Algorithm
- Q6) C
Relates to: Configuring Single Area OSPF
- Q7) D
Relates to: Configuring Single Area OSPF
- Q8) C
Relates to: Verifying the OSPF Configuration
- Q9) B
Relates to: Verifying the OSPF Configuration
- Q10) A
Relates to: Troubleshooting the OSPF Configuration
- Q11) D
Relates to: Troubleshooting the OSPF Configuration

Variable-Length Subnet Masks

Overview

Variable-length subnet masks (VLSMs) were developed to allow multiple levels of subnetted IP addresses within a single network. This strategy can be used only when it is supported by the routing protocol in use, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP). This lesson introduces the capabilities provided by VLSMs.

Relevance

VLSM is a key technology on large routed networks. Understanding its capabilities is important when planning large networks.

Objectives

Upon completing this lesson, you will be able to:

- Explain the operation of variable-length subnet masks on Cisco routers

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

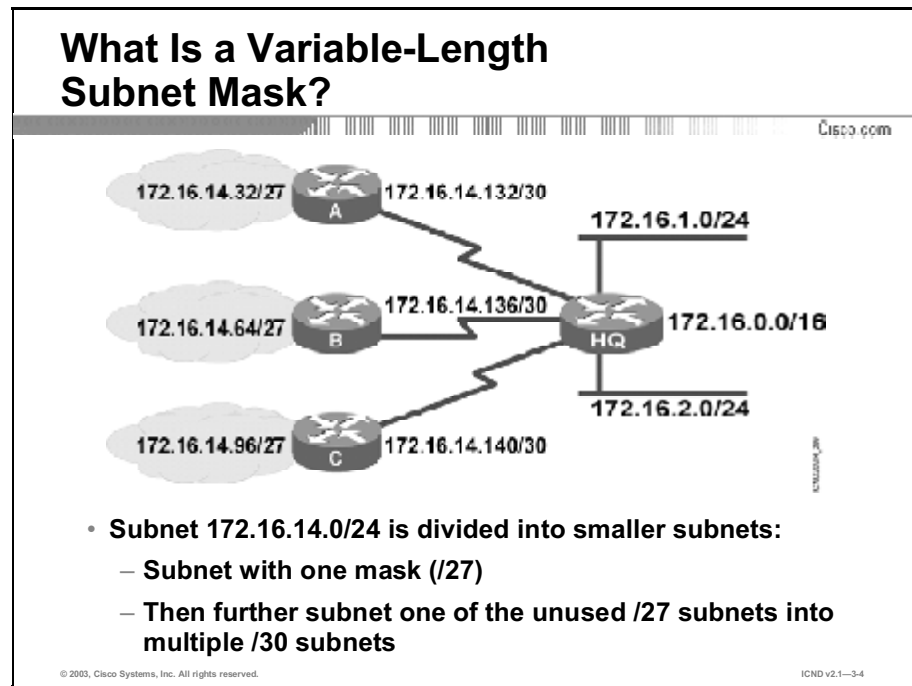
Outline

The lesson includes these topics:

- Overview
- VLSM Features
- Route Summarization with VLSM
- Summary
- Quiz

VLSM Features

When an IP network is assigned more than one subnet mask, it is considered a network with variable-length subnet masks (VLSMs), overcoming the limitation of a fixed number of fixed-size subnetworks that are imposed by a single subnet mask. This topic describes the features of variable-length subnet masks.



VLSMs provide the ability to include more than one subnet mask within a network and the ability to subnet an already subnetted network address. VLSM offers the following benefits:

- **Even more efficient use of IP addresses:** Without the use of VLSMs, companies must implement a single subnet mask within an entire class A, B, or C network number.

For example, consider the 172.16.0.0/16 network address divided into subnets using /24 masking, and one of the subnetworks in this range, 172.16.14.0/24, further divided into smaller subnets with the /27 masking, as shown in the figure. These smaller subnets range from 172.16.14.0/27 to 172.16.14.224/27. In the figure, one of these smaller subnets, 172.16.14.128/27, is further divided with the /30 prefix, creating subnets with only two hosts, to be used on the WAN links. The /30 subnets range from 172.16.14.128/30 to 172.16.14.156/30. In the figure, the WAN links used the 172.16.14.132/30, 172.16.14.136/30, and 172.16.14.140/30 subnets out of the range.

- **Greater capability to use route summarization:** VLSM allows more hierarchical levels within an addressing plan, and thus allows better route summarization within routing tables. For example, in the figure, subnet 172.16.14.0/24 summarizes all of the addresses that are further subnets of 172.16.14.0, including those from subnet 172.16.14.0/27 and from 172.16.14.128/30.

Calculating VLSMs

Cisco.com

Subnetted Address: 172.16.32.0/20

In Binary 10101100.00010000.00100000.00000000

VLSM Address: 172.16.32.0/26

In Binary 10101100.00010000.00100000.00000000

1st subnet:	172	.	16	.	0010	0000.00	000000=172.16.32.0/26
2nd subnet:	172	.	16	.	.0010	0000.01	000000=172.16.32.64/26
3rd subnet:	172	.	16	.	.0010	0000.10	000000=172.16.32.128/26
4th subnet:	172	.	16	.	.0010	0000.11	000000=172.16.32.192/26
5th subnet:	172	.	16	.	.0010	001.00	000000=172.16.33.0/26
	Network			Subnet	VLSM	Host	
					Subnet		

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-5

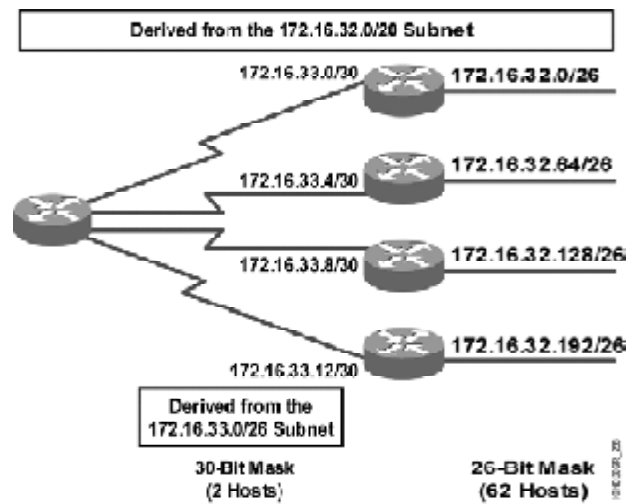
As discussed, with VLSMs you can subnet an already subnetted address. Consider, for example, that you have a subnet address 172.16.32.0/20, and you need to assign addresses to a network that has ten hosts. With this subnet address, however, you have over 4000 ($2^{12} - 2 = 4094$) host addresses, most of which will be wasted. With VLSMs you can further subnet the address 172.16.32.0/20 to give you more network addresses and fewer hosts per network. If, for example, you subnet 172.16.32.0/20 to 172.16.32.0/26, you gain 64 (2^6) subnets, each of which could support 62 ($2^6 - 2$) hosts.

Use this procedure to further subnet 172.16.32.0/20 to 172.16.32.0/26:

- Step 1** Write 172.16.32.0 in binary form.
- Step 2** Draw a vertical line between the 20th and 21st bits, as shown in the figure. (/20 was the original subnet boundary.)
- Step 3** Draw a vertical line between the 26th and 27th bits, as shown in the figure. (The original /20 subnet boundary is extended six bits to the right, becoming /26.)
- Step 4** Calculate the 64 subnet addresses using the bits between the two vertical lines, from lowest to highest in value. The figure shows the first five subnets available.

A Working VLSM Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-6

VLSMs are commonly used to maximize the number of possible addresses available for a network. For example, because point-to-point serial lines require only two host addresses, using a /30 subnet will not waste scarce IP addresses.

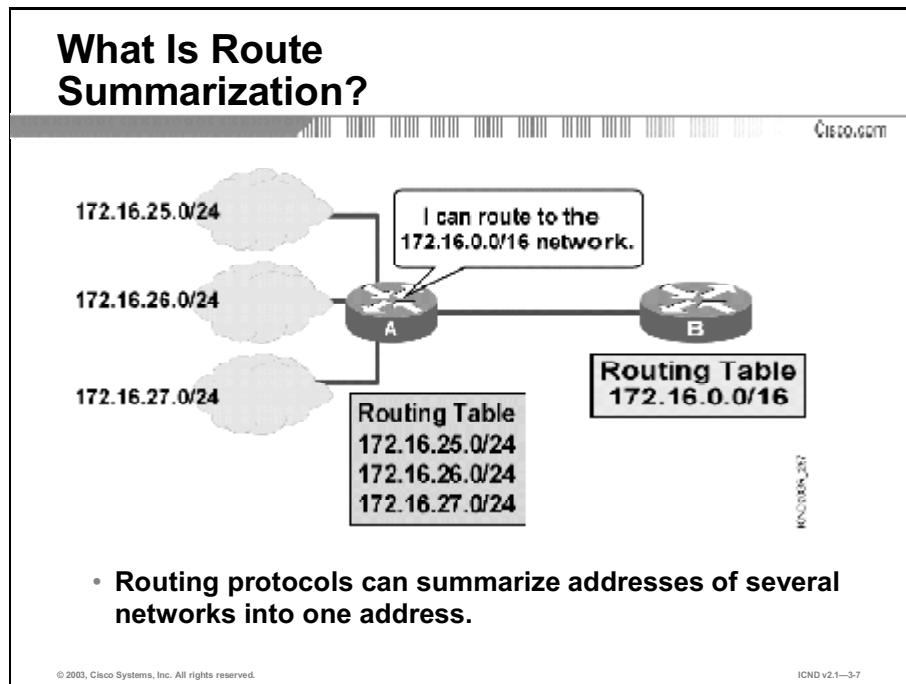
In the figure, the subnet addresses used on the Ethernets are those generated from subdividing the 172.16.32.0/20 subnet into multiple /26 subnets. The figure illustrates where the subnet addresses can be applied, depending on the number of host requirements. For example, the WAN links use subnet addresses with a prefix of /30. This prefix allows for only two hosts: just enough hosts for a point-to-point connection between a pair of routers.

To calculate the subnet addresses used on the WAN links, further subnet one of the unused /26 subnets. In this example, 172.16.33.0/26 is further subnetted with a prefix of /30. This provides four more subnet bits and therefore 16 (2^4) subnets for the WANs.

Note It is important to remember that only unused subnets can be further subnetted. In other words, if you use any addresses from a subnet, that subnet cannot be further subnetted. In the example, four subnet numbers are used on the LANs. Another unused subnet, 172.16.33.0/26, is further subnetted for use on the WANs.

Route Summarization with VLSM

In large internetworks, hundreds or even thousands of network addresses can exist. In these environments, it is often not desirable for routers to maintain many routes in their routing table. Route summarization, also called route aggregation or supernetting, can reduce the number of routes that a router must maintain by representing a series of network numbers in a single summary address. This topic describes and gives examples of route summarization, including implementation considerations.



For example, as shown in the figure, router A can either send three routing update entries or summarize the addresses into a single network number. The figure illustrates a summary route based on a full octet: 172.16.25.0/24, 172.16.26.0/24, and 172.16.27.0/24 could be summarized into 172.16.0.0/16.

Note The router in the figure can route to network 172.16.0.0/16, including all subnets of that network. However, if there were other subnets of 172.16.0.0 elsewhere in the network (for example, if 172.16.0.0 was discontinuous), summarizing in this way may not be valid. Discontinuous networks and summarization are discussed later in this lesson.

Another advantage to using route summarization in a large, complex network is that it can isolate topology changes from other routers. That is, if a specific link in the 172.16.27.0/24 domain was “flapping,” or going up and down rapidly, the summary route would not change. Therefore, no router external to the domain would need to keep modifying its routing table due to this flapping activity.

Route summarization is most effective within a subnetted environment when the network addresses are in contiguous blocks in powers of two. For example, 4, 16, or 512 addresses can be represented by a single routing entry because summary masks are binary masks—just like subnet masks—so summarization must take place on binary boundaries (powers of two).

Routing protocols summarize or aggregate routes based on shared network numbers within the network. Classless routing protocols, such as Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Enhanced Interior Gateway Routing Protocol (EIGRP), support route summarization based on subnet addresses, including VLSM addressing. Classful routing protocols, such as RIPv1 and Interior Gateway Routing Protocol (IGRP), automatically summarize routes on the classful network boundary, and do not support summarization on any other boundaries.

Note	Summarization is described in RFC 1518, "An Architecture for IP Address Allocation with CIDR."

Summarizing Within an Octet

Cisco.com

172.16.168.0/24 =	10101100	.	00010000	.	10101	000	.	00000000
172.16.169.0/24 =	172	.	16	.	10101	001	.	0
172.16.170.0/24 =	172	.	16	.	10101	010	.	0
172.16.171.0/24 =	172	.	16	.	10101	011	.	0
172.16.172.0/24 =	172	.	16	.	10101	100	.	0
172.16.173.0/24 =	172	.	16	.	10101	101	.	0
172.16.174.0/24 =	172	.	16	.	10101	110	.	0
172.16.175.0/24 =	172	.	16	.	10101	111	.	0

Number of Common Bits = 21
Summary: 172.16.168.0/21

Noncommon
Bits = 11

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-8

Suppose a router receives updates for the following routes:

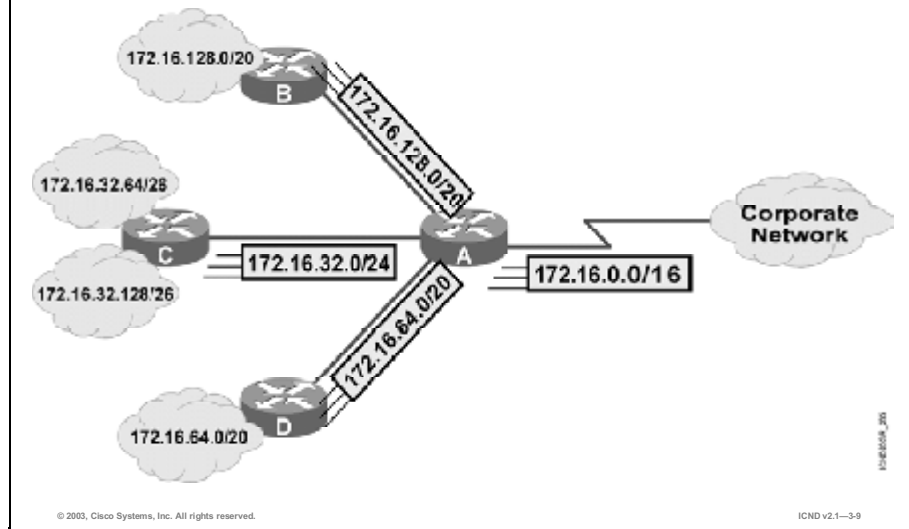
- 172.16.168.0/24
- 172.16.169.0/24
- 172.16.170.0/24
- 172.16.171.0/24
- 172.16.172.0/24
- 172.16.173.0/24
- 172.16.174.0/24
- 172.16.175.0/24

To determine the summary route, the router determines the number of highest-order bits that match in all of the addresses. By converting the IP addresses to the binary format, you can determine the number of common bits shared among the IP addresses. In the figure, the first 21 bits are in common among the IP addresses. Therefore, the best summary route is 172.16.168.0/21. You can summarize addresses when the number of addresses is a power of two. If the number of addresses is not a power of two, you can divide the addresses into groups and summarize the groups separately.

To allow the router to aggregate the most number of IP addresses into a single route summary, your IP addressing plan should be hierarchical in nature. This approach is particularly important when using VLSMs.

Summarizing Addresses in a VLSM-Designed Network

Cisco.com



A VLSM design allows for maximum use of IP addresses, as well as more efficient routing update communication when using hierarchical IP addressing. In the figure, for example, route summarization occurs at two levels:

- Router C summarizes two routing updates from networks 172.16.32.64/26 and 172.16.32.128/26 into a single update, 172.16.32.0/24.
- Router A receives three different routing updates but summarizes them into a single routing update before propagating it to the corporate network.

Implementation Considerations

Cisco.com

- **Multiple IP addresses must have the same highest-order bits.**
- **Routing decisions are made based on the entire address.**
- **Routing protocols must carry the prefix (subnet mask) length.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-10

Route summarization reduces memory use on routers and routing protocol network traffic. Requirements for summarization to work correctly are as follows:

- Multiple IP addresses must share the same highest-order bits.
- Routing protocols must base their routing decisions on a 32-bit IP address and a prefix length that can be up to 32 bits.
- Routing protocols must carry the prefix length (subnet mask) with the 32-bit IP address.

Route Summarization Operation in Cisco Routers

Cisco.com

192.16.5.33	/32	Host
192.16.5.32	/27	Subnet
192.16.5.0	/24	Network
192.16.0.0	/16	Block of Networks
0.0.0.0	/0	Default

- **Supports host-specific routes, blocks of networks, default routes.**
- **Routers use the longest match.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-11

Cisco routers manage route summarization in two ways, as follows:

- **Sending route summaries:** Routing protocols like RIP, IGRP, and EIGRP perform automatic route summarization across network boundaries. Specifically, this automatic summarization occurs for those routes whose classful network address differs from the major network address of the interface to which the advertisement is being sent. For OSPF and IS-IS, you must configure manual summarization. For EIGRP and RIPv2, you can disable automatic route summarization and configure manual summarization. Whether routing summarization is automatic or not is dependent on the routing protocol. It is recommended that you review the documentation for your specific routing protocols.

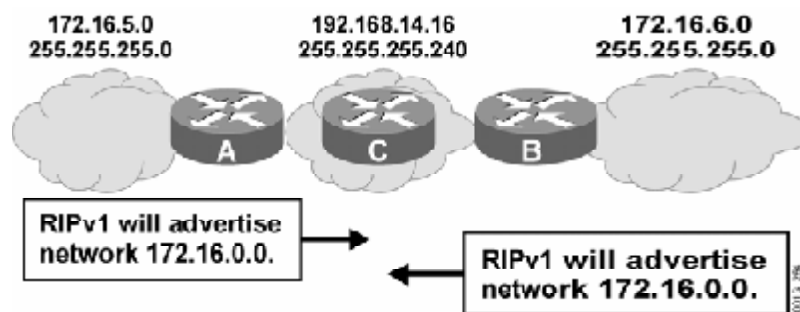
Route summarization is not always a solution. You would not use route summarization if you needed to advertise all networks across a boundary, such as when you have discontinuous networks.

- **Selecting routes from route summaries:** If more than one entry in the routing table matches a particular destination, the longest prefix match in the routing table is used. Several routes might match one destination, but the longest matching prefix is used.

For example, if a routing table has different paths to 192.16.0.0/16 and to 192.16.5.0/24, packets addressed to 192.16.5.99 would be routed through the 192.16.5.0/24 path because that address has the longest match with the destination address.

Summarizing Routes in a Discontiguous Network

Cisco.com



- RIPv1 and IGRP do not advertise subnets, and therefore cannot support discontiguous subnets.
- OSPF, EIGRP, and RIPv2 can advertise subnets, and therefore can support discontiguous subnets.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—3-12

Classful routing protocols summarize automatically at network boundaries. This behavior, which cannot be changed with RIPv1 and IGRP, has important results, as follows:

- Subnets are not advertised to a different major network.
- Discontiguous subnets are not visible to each other.

In the example, RIPv1 does not advertise the 172.16.5.0 255.255.255.0 and 172.16.6.0 255.255.255.0 subnets because RIPv1 cannot advertise subnets; both router A and router B advertise 172.16.0.0. This leads to confusion when routing across network 192.168.14.0. In this example, router C receives routes about 172.16.0.0 from two different directions, so it cannot make a correct routing decision.

You can resolve this situation by using RIPv2, OSPF, IS-IS, or EIGRP and *not* using summarization, because the subnet routes would be advertised with their actual subnet masks.

Cisco IOS software also provides an IP unnumbered feature that permits discontiguous subnets to be separated by an unnumbered link.

Summary

This topic summarizes the key points discussed this lesson.

Summary



- **When an IP network is assigned more than one subnet mask, it is considered a network with variable-length subnet masks, overcoming the limitation of a fixed number of fixed-size subnetworks imposed by a single subnet mask.**
- **In large internetworks, hundreds or even thousands of network addresses can exist. In these environments, it is often not desirable for routers to maintain many routes in their routing table. Route summarization, also called route aggregation or supernetting, can reduce the number of routes that a router must maintain by representing a series of network numbers in a single summary address.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—3-13

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Next Steps

After completing this lesson, go to:

- Lab Exercise 3-1: Determining IP Routes with RIP
- Lab Exercise 3-2: Determining IP Routes with IGRP
- Lab Exercise 3-3: Determining IP Routes with EIGRP
- Lab Exercise 3-4: Determining IP Routes with OSPF

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which two addresses are valid subnet addresses when 172.17.15.0/24 is subnetted an additional four bits? (Choose two.)
- A) 172.17.15.0
 - B) 172.17.15.8
 - C) 172.17.15.40
 - D) 172.17.15.96
 - E) 172.17.15.248
- Q2) What is the most efficient subnet mask to use on point-to-point WAN links?
- A) 255.255.255.0
 - B) 255.255.255.224
 - C) 255.255.255.252
 - D) 255.255.255.255
- Q3) Which two terms are alternatives for route summarization? (Choose two.)
- A) CIDR
 - B) VLSM
 - C) subnetting
 - D) aggregation
 - E) supernetting
- Q4) What is the best summary route for the addresses 172.17.192.0/24 through 172.17.207.0/24?
- A) 172.17.0.0/16
 - B) 172.17.192.0/20
 - C) 172.17.192.0/24
 - D) 172.17.207.0/24

Quiz Answer Key

Q1) A, D

Relates to: VLSM Features

Q2) C

Relates to: VLSM Features

Q3) D, E

Relates to: Route Summarization with VLSM

Q4) B

Relates to: Route Summarization with VLSM

Lesson Assessments

Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

Outline

This section includes these assessments:

- Lesson Assessment 3-1: Routing Overview
- Lesson Assessment 3-2: Distance Vector Routing
- Lesson Assessment 3-3: Link-State and Balanced Hybrid Routing
- Lesson Assessment 3-4: Enabling RIP
- Lesson Assessment 3-5: Enabling IGRP
- Lesson Assessment 3-6: Enabling EIGRP
- Lesson Assessment 3-7: Enabling OSPF
- Lesson Assessment 3-8: Variable-Length Subnet Masks

Lesson Assessment 3-1: Routing Overview

Complete this quiz to assess what you have learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Explain the differences between static routing and dynamic routing
- Identify the classes of routing protocols
- Use Cisco IOS commands to configure static routes and default route forwarding, given a functioning router
- Use **show** commands to identify anomalies in static routing operation, given an operational router
- Describe the operation of “router on a stick”
- Configure router on a stick for interVLAN routing using ISL or 802.1Q trunking, given an operational switch and router

Quiz

Answer these questions:

- Q1) Using dynamic routing, which two tasks must a router perform to route traffic?
(Choose two.)
- A) discover routes
 - B) classify the data being sent
 - C) identify sources of routing information
 - D) determine the source address of each packet to be routed
- Q2) Which statement most accurately describes static and dynamic routes?
- A) Dynamic routes are manually configured by a network administrator while static routes are automatically learned and adjusted by a routing protocol.
 - B) Static routes are manually configured by a network administrator while dynamic routes are automatically learned and adjusted by a routing protocol.
 - C) Static routes tell the router how to forward packets to networks that are not directly connected while dynamic routes tell the router how to forward packets to networks that are directly connected.
 - D) Dynamic routes tell the router how to forward packets to networks that are not directly connected while static routes tell the router how to forward packets to networks that are directly connected.
- Q3) A stub network is a network ____.
- A) that is accessible by only one path
 - B) where dynamic routes are usually used
 - C) with the stub command configured on all devices
 - D) that is accessible by multiple paths, but all of equal cost

- Q4) Which command correctly specifies that traffic for destination network 192.168.45.0 should be sent to address 10.2.2.2?
- A) **ip route 192.168.45.0 10.2.2.2 255.255.255.0**
 - B) **ip route 192.168.45.0 255.255.255.0 10.2.2.2**
 - C) **ip route 10.2.2.2 255.255.255.0 192.168.45.0**
 - D) **ip route 255.255.255.0 192.168.45.0 10.2.2.2**
- Q5) What does the command `ip route 186.157.5.0 255.255.255.0 10.1.1.3` specify?
- A) Both 186.157.5.0 and 10.1.1.3 use a mask of 255.255.255.0
 - B) The router should use network 186.157.5.0 to get to address 10.1.1.3
 - C) You want the router to trace a route to network 186.157.5.0 via 10.1.1.3
 - D) The router should use address 10.1.1.3 to get to devices on network 186.157.5.0
- Q6) Which command correctly designates 10.2.2.4 as the next hop for the default route?
- A) **ip route 0.0.0.0 10.2.2.4**
 - B) **ip route 10.2.2.4 0.0.0.0 0.0.0.0**
 - C) **ip route 0.0.0.0 10.2.2.4 0.0.0.0**
 - D) **ip route 0.0.0.0 0.0.0.0 10.2.2.4**
 - E) **ip route 255.255.255.255 255.255.255.255 10.2.2.4**
- Q7) Which command displays information about static route configuration on a Cisco router?
- A) **show route ip**
 - B) **show ip route**
 - C) **show ip route static**
 - D) **show route ip static**
- Q8) What is a class of routing protocol that combines aspects of the link-state and distance vector algorithms?
- A) mix
 - B) hybrid
 - C) link distance
 - D) distance link
- Q9) What is an example of an exterior gateway protocol?
- A) RIP
 - B) BGP
 - C) IGRP
 - D) EIGRP

- Q10) In which situation is an administrative distance required?
- A) whenever static routes are defined
 - B) whenever dynamic routing is enabled
 - C) when the same route is learned via multiple routing protocols
 - D) when there are multiple paths available to the same destination and they are all learned via the same routing protocol
- Q11) Which routing protocol has a default administrative distance of 120 on Cisco routers?
- A) RIP
 - B) OSPF
 - C) IGRP
 - D) EIGRP
- Q12) When a router receives a packet with a destination address that is within an unknown subnet of a directly attached network, what is the default behavior if **ip classless** is not enabled?
- A) drop the packet
 - B) forward the packet to the default route
 - C) forward the packet to the next hop for the directly attached network
 - D) broadcast the packet through all interfaces except the one on which it was received
- Q13) Which command correctly ensures that if the router receives any packets for which it does not have an explicit route, it will send the packets to the default route?
- A) Router(config)#**classless**
 - B) Router(config)#**ip classless**
 - C) Router(config-router)#**classless routing**
 - D) Router(config-router)# **ip classless routing**
- Q14) Besides enabling ISL trunking on subinterfaces, what step must you perform on the router to enable “router on a stick”?
- A) assign each subinterface to a network
 - B) assign an IP address to each subinterface
 - C) assign a MAC address to each subinterface
 - D) assign a network number to each subinterface
- Q15) Which command correctly assigns a subinterface to VLAN 50 using 802.1Q trunking?
- A) Router(config)#**encapsulation 50 dot1Q**
 - B) Router(config)#**encapsulation 802.1Q 50**
 - C) Router(config-if)#**encapsulation dot1Q 50**
 - D) Router(config-if)#**encapsulation 50 802.1Q**

- Q16) Which command correctly assigns a subinterface to VLAN 50 using ISL trunking?
- A) Router(config)#**encapsulation isl 50**
 - B) Router(config)#**encapsulation 50 isl**
 - C) Router(config-if)#**encapsulation isl 50**
 - D) Router(config-if)#**encapsulation 50 isl**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-2: Distance Vector Routing

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features offered by distance vector routing protocols and give examples of each
- Describe the issues associated with distance vector routing and identify solutions to those issues

Quiz

Answer these questions:

- Q1) How does a distance vector router learn about paths for networks that are not directly connected?
- A) From the source router.
 - B) From neighboring routers.
 - C) From the destination router.
 - D) Distance vector routers only learn about directly connected networks.
- Q2) What does a distance vector router send to its neighbor routers as part of a periodic routing table update?
- A) the entire routing table
 - B) information about new routes
 - C) information about routes that have changed
 - D) information about routes that no longer exist
- Q3) Which metric is used by distance vector routing algorithms?
- A) cost
 - B) hop count
 - C) bandwidth
 - D) depends on the routing protocol
- Q4) A routing loop is the term that is used to specify which problem?
- A) Packets that are sent to a particular destination are returned to their source.
 - B) Packets that are sent to a particular destination bounce continuously between routers.
 - C) The metric for a particular route rotates through two or more values continuously.
 - D) The metric for a particular route is increased indefinitely through repeated routing table updates.

- Q5) With distance vector routing, the administrator can prevent count to infinity by setting a maximum for what value?
- A) metric
 - B) update time
 - C) holddown time
 - D) administrative distance
- Q6) What does split horizon specify?
- A) that information about a route should not be sent in any direction
 - B) that information about a route should not be sent back in the direction from which the original information came
 - C) that information about a route should always be sent back in the direction from which the original information came
 - D) that information about a route should only be sent back in the direction from which the original information came
- Q7) When a router sets the metric for a network that has gone down to the maximum value, what is it doing?
- A) triggering the route
 - B) poisoning the route
 - C) applying split horizon
 - D) putting the route in holddown
- Q8) When is a triggered update sent?
- A) when the flush timer expires
 - B) when the holddown timer expires
 - C) at the same time as periodic updates
 - D) immediately, in response to a topology change
- Q9) If a route for a network is in holddown and an update arrives from a neighboring router with the same metric as was originally recorded for the network, what does the router do?
- A) ignores the update
 - B) increments the holddown timer
 - C) marks the network as accessible and removes the holddown timer
 - D) marks the network as accessible but keeps the holddown timer on
- Q10) If a router has a network path in holddown and an update arrives from a neighboring router with a better metric than originally recorded for the network, what two things does it do? (Choose two.)
- A) removes the holddown
 - B) continues the holddown
 - C) marks the route as accessible
 - D) marks the route as inaccessible
 - E) marks the route as possibly down

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-3: Link-State and Balanced Hybrid Routing

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the issues associated with link-state routing and identify solutions to those issues
- Describe the features of balanced hybrid routing protocols

Quiz

Answer these questions:

- Q1) What type of routing protocol is OSPF?
- A) static
 - B) link-state
 - C) distance vector
 - D) balanced hybrid
- Q2) How can link-state protocols limit the scope of route changes?
- A) by supporting classless addressing
 - B) by sending the mask along with the address
 - C) by sending only updates of a topology change
 - D) by segmenting the network into area hierarchies
- Q3) What is the purpose of link-state advertisements?
- A) to construct a topological database
 - B) to specify the cost to reach a destination
 - C) to determine the best path to a destination
 - D) to verify that a neighbor is still functioning
- Q4) How are balanced hybrid protocols like link-state protocols?
- A) faster convergence
 - B) both use the same metrics
 - C) both use the Dijkstra algorithm
 - D) both use frequent periodic routing updates
- Q5) What type of routing protocol is EIGRP?
- A) static
 - B) link-state
 - C) distance vector
 - D) balanced hybrid

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-4: Enabling RIP

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of RIP
- Use Cisco IOS commands to configure dynamic routing using RIP, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using RIP, given an operational router

Quiz

Answer these questions:

- Q1) By default, how often does RIP broadcast routing updates?
- A) every 6 seconds
 - B) every 15 seconds
 - C) every 30 seconds
 - D) every 60 seconds
- Q2) What is the maximum allowable hop count for RIP?
- A) 6
 - B) 15
 - C) 30
 - D) 60
- Q3) With RIP, load balancing is performed over multiple paths with what characteristic?
- A) equal cost
 - B) equal weight
 - C) equal distance
 - D) equal bandwidth
- Q4) Router D has three interfaces as follows:
- E0: 10.1.1.5
E1: 10.1.2.6
S0: 192.168.2.1
- Which configuration is required to specify that RIP is to run on all of the router D interfaces?
- A) network 10.0.0.0
 - B) network 10.0.0.0, network 192.168.0.0
 - C) network 10.1.1.0, network 10.1.2.0, network 192.168.2.0
 - D) network 10.1.1.5, network 10.1.2.6, network 192.168.2.1

- Q5) Which command correctly specifies RIP as the routing protocol?
- A) Router(config)#**rip**
 - B) Router(config)#**router rip**
 - C) Router(config-router)#**rip {AS no.}**
 - D) Router(config-router)#**router rip {AS no.}**
- Q6) What is the default value of the RIP holddown timer?
- A) 30 seconds
 - B) 60 seconds
 - C) 90 seconds
 - D) 180 seconds
- Q7) In this line from the output of the **debug ip rip** command, what is the number in parentheses?
- RIP: sending v1 update to 255.255.255.255 via Ethernet1 (10.1.1.2)
- A) the source address
 - B) the next-hop address
 - C) the destination address
 - D) the address of the routing table entry
- Q8) What could cause the message “RIP: bad version 128 from 160.89.80.43” to be displayed in the output of the **debug ip rip** command?
- A) receiving a malformed packet
 - B) sending a routing table update
 - C) receiving a routing table update
 - D) manually clearing the routing table

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-5: Enabling IGRP

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of IGRP
- Use Cisco IOS commands to configure dynamic routing using IGRP, given a functioning router
- Use **show** commands to identify anomalies in dynamic routing operation using IGRP, given an operational router

Quiz

Answer these questions:

- Q1) Which two factors can be included in an IGRP composite routing metric? (Choose two.)
- A) load
 - B) distance
 - C) reliability
 - D) hop count
 - E) CPU speed
- Q2) Which two features are advantages of IGRP over RIP? (Choose two.)
- A) scalability
 - B) simplicity
 - C) convergence
 - D) multiple paths
 - E) multiple unequal paths
- Q3) What advantage does the IGRP composite metric have over the RIP hop count metric?
- A) faster speed
 - B) greater accuracy
 - C) greater simplicity
 - D) faster convergence
- Q4) Which two components of the IGRP composite metric are not used by default? (Choose two.)
- A) delay
 - B) loading
 - C) flexibility
 - D) bandwidth
 - E) MTU value

- Q5) With the IGRP unequal-cost path load balancing, why must the next-hop router of each alternate path be closer to the destination than the local router by its best path?
- A) to ensure scalability
 - B) to ensure packet arrival
 - C) to prevent routing loops
 - D) to prevent multiple packet distribution
- Q6) With IGRP load balancing, if the metric for an alternative path is twice the metric for the best path, how often will the alternative path be used compared to the best path?
- A) never
 - B) just as often
 - C) half as often
 - D) twice as often
- Q7) Which command will distribute traffic across IGRP multiple paths only to the paths with the lowest metric (equal cost paths load balancing)?
- A) **variance 2**
 - B) **traffic-share min**
 - C) **traffic-share balanced**
 - D) **traffic-share variance 1**
- Q8) With IGRP load balancing, which command specifies that the metric of a feasible alternate path to a destination can be no more than three times the metric of the best path metric to that destination?
- A) **variance 3**
 - B) **variance 0.3**
 - C) **traffic-share min**
 - D) **traffic-share balanced**
- Q9) The flush value, as displayed in the output of the **show ip protocols** command, should be greater than the sum of which two other values?
- A) update and invalid
 - B) update and holddown
 - C) invalid and holddown
 - D) invalid and twice holddown
- Q10) In the output of the **show ip protocols** command, what is represented by the number in the line "Routing protocol is 'igrp 10'"?
- A) interface number
 - B) maximum hop count
 - C) major network number
 - D) autonomous system number

- Q11) Which command displays a count of the routes contained in an IGRP update?
- A) **debug ip igrp events**
 - B) **debug ip igrp transactions**
 - C) **debug ip igrp events summary**
 - D) **debug ip igrp transactions summary**
- Q12) If router A sends router B an IGRP update indicating that a route that was inaccessible is now reachable, when will router B update its routing table?
- A) immediately
 - B) after 10 seconds
 - C) when it receives a second notice
 - D) when the holddown timer expires
- Q13) Which command displays metric information contained in an IGRP update?
- A) **debug ip igrp events**
 - B) **debug ip igrp transactions**
 - C) **debug ip igrp events summary**
 - D) **debug ip igrp transactions summary**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-6: Enabling EIGRP

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of EIGRP
- Use Cisco IOS commands to configure dynamic routing using EIGRP, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using EIGRP, given an operational router

Quiz

Answer these questions:

- Q1) How is the bandwidth requirement for EIGRP packets minimized?
- A) by propagating only data packets
 - B) by propagating only hello packets
 - C) by propagating only routing table changes and hello packets
 - D) by propagating the entire routing table only to those routers affected by a topology change
- Q2) Which two features have been improved in EIGRP over IGRP? (Choose two.)
- A) composite metric
 - B) hop count metric
 - C) faster convergence time
 - D) lower network overhead
 - E) unequal-cost load balancing
- Q3) In the command **router eigrp 77**, what is indicated by the number 77?
- A) variance
 - B) major network number
 - C) autonomous system number
 - D) number of EIGRP processes to run
- Q4) Which command correctly specifies that network 10.0.0.0 is directly connected to a router running EIGRP?
- A) Router(config)#**network 10.0.0.0**
 - B) Router(config)#**router eigrp 10.0.0.0**
 - C) Router(config-router)#**network 10.0.0.0**
 - D) Router(config-router)#**router eigrp 10.0.0.0**

- Q5) Which command displays the amount of time since the router heard from an EIGRP neighbor?
- A) **show ip eigrp traffic**
 - B) **show ip eigrp topology**
 - C) **show ip eigrp interfaces**
 - D) **show ip eigrp neighbors**
- Q6) In the output of the **debug ip eigrp** command, what is specified by the 130560 in “M 386560 – 256000 130560”?
- A) delay
 - B) computed metric
 - C) inverse bandwidth
 - D) metric advertised by the neighbor
- Q7) Which label specifies the calculated metric in the output of the **debug ip eigrp** command?
- A) M
 - B) SM
 - C) Int
 - D) Ext

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-7: Enabling OSPF

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of the OSPF protocol
- Use Cisco IOS commands to configure dynamic routing for a single area OSPF network, given a functioning router
- Use **show** and **debug** commands to identify anomalies in dynamic routing operation using OSPF, given an operational router

Quiz

Answer these questions:

- Q1) What are two characteristics of OSPF? (Choose two.)
- A) IGP
 - B) proprietary
 - C) open standard
 - D) similar to RIP
 - E) distance vector protocol
- Q2) OSPF routes packets within a single ____.
- A) area
 - B) network
 - C) segment
 - D) autonomous system
- Q3) What two pieces of information are included in a link-state advertisement? (Choose two.)
- A) uptime
 - B) hop count
 - C) metrics used
 - D) MAC address
 - E) attached interfaces
- Q4) In link-state protocols, ____ can be divided into a number of ____.
- A) an area; autonomous systems
 - B) an autonomous system; areas
 - C) an area; contiguous networks
 - D) an autonomous system; contiguous networks

- Q5) A link-state database is also called a _____ database.
- A) logical
 - B) topological
 - C) geographical
 - D) MAC address
- Q6) With OSPF, each router builds its SPF tree using the same link-state information, but each will have a separate _____ of the topology.
- A) state
 - B) view
 - C) version
 - D) configuration
- Q7) What component of the SPF algorithm is inversely proportional to bandwidth?
- A) link cost
 - B) root cost
 - C) link state
 - D) hop count
- Q8) Which command correctly starts an OSPF routing process using process-ID 191?
- A) Router(config)#**router ospf 191**
 - B) Router(config)#**network ospf 191**
 - C) Router(config-router)#**network ospf 191**
 - D) Router(config-router)#**router ospf process-id 191**
- Q9) In the command **network 198.172.0.0 0.0.255.255 area 0**, what is specified by “0.0.255.255”?
- A) that the last octet of IP addresses needs to match the specified address
 - B) that the first octet of IP addresses needs to match the specified address
 - C) that the last two octets of IP addresses need to match the specified address
 - D) that the first two octets of IP addresses need to match the specified address
- Q10) How many host addresses are useable when using a /29 mask with VLSM?
- A) 6
 - B) 8
 - C) 14
 - D) 16
- Q11) Which mask borrows four bits of the host part of the class C address for the network part?
- A) /26
 - B) /27
 - C) /28
 - D) /29

- Q12) What is the first step of subnetting with VLSM?
- A) determining the physical location of each subnet
 - B) determining the range of addresses for each subnet
 - C) determining the number of hosts required for each subnet
 - D) determining the power of two that will provide the correct number of hosts
- Q13) Which network address is equivalent to the one assigned with **ip address 192.168.53.16 255.255.255.240** ?
- A) 192.168.53.16/26
 - B) 192.168.53.16/27
 - C) 192.168.53.16/28
 - D) 192.168.53.16/29
- Q14) What is the purpose of the **show ip ospf interface** command?
- A) to display OSPF-related interface information
 - B) to display general information about OSPF routing processes
 - C) to display OSPF neighbor information on a per-interface basis
 - D) to display OSPF neighbor information on a per-interface type basis
- Q15) Which number in the OSPF authentication type field of the output from the **debug ip ospf packet** command indicates a simple password?
- A) 0
 - B) 1
 - C) 2
 - D) 3
- Q16) The output from which command includes information about the length of the OSPF packet?
- A) **debug ip ospf events**
 - B) **debug ip ospf packet**
 - C) **debug ip ospf packet size**
 - D) **debug ip ospf mpls traffic-eng advertisements**
- Q17) In the output of the **debug ip ospf packet** command, which label is used to identify the OSPF area ID?
- A) rid
 - B) aid
 - C) chk
 - D) auk

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 3-8: Variable-Length Subnet Masks

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Explain the operation of variable-length subnet masking on Cisco routers

Quiz

Answer these questions:

- Q1) How many subnets are gained by subnetting 172.17.32.0/20 into multiple /28 subnets?
- A) 16
 - B) 32
 - C) 256
 - D) 1024
- Q2) How many hosts can be addressed on a subnet with seven host bits?
- A) 7
 - B) 62
 - C) 126
 - D) 252
- Q3) How many hosts can be addressed with a prefix of /30?
- A) 1
 - B) 2
 - C) 4
 - D) 30
- Q4) Which subnet mask would be appropriate for a class C address used for 9 LANs, each with 12 hosts?
- A) 255.255.255.0
 - B) 255.255.255.224
 - C) 255.255.255.240
 - D) 255.255.255.252

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment Answer Key

Lesson Assessment 3-1: Routing Overview

- Q1) A, C
- Q2) B
- Q3) A
- Q4) B
- Q5) D
- Q6) D
- Q7) B
- Q8) B
- Q9) B
- Q10) C
- Q11) A
- Q12) A
- Q13) B
- Q14) B
- Q15) C
- Q16) C

Lesson Assessment 3-2: Distance Vector Routing

- Q1) B
- Q2) A
- Q3) D
- Q4) B
- Q5) A
- Q6) B
- Q7) B
- Q8) D
- Q9) A
- Q10) A, C

Lesson Assessment 3-3: Link-State and Balanced Hybrid Routing

- Q1) B
- Q2) D
- Q3) A
- Q4) A
- Q5) D

Lesson Assessment 3-4: Enabling RIP

- Q1) C
- Q2) B
- Q3) A
- Q4) B
- Q5) B
- Q6) D
- Q7) A
- Q8) A

Lesson Assessment 3-5: Enabling IGRP

- Q1) A, C
- Q2) A, E
- Q3) B
- Q4) B, E
- Q5) C
- Q6) C
- Q7) B
- Q8) A
- Q9) C
- Q10) D
- Q11) A
- Q12) D
- Q13) B

Lesson Assessment 3-6: Enabling EIGRP

- Q1) C
- Q2) C, D
- Q3) C
- Q4) C
- Q5) D
- Q6) A
- Q7) A

Lesson Assessment 3-7: Enabling OSPF

- Q1) C
- Q2) D
- Q3) C, E
- Q4) B
- Q5) B
- Q6) B
- Q7) A
- Q8) A
- Q9) D
- Q10) A
- Q11) C
- Q12) C
- Q13) C
- Q14) A
- Q15) B
- Q16) B
- Q17) B

Lesson Assessment 3-8: Variable-Length Subnet Masks

- Q1) C
- Q2) C
- Q3) B
- Q4) C

Managing IP Traffic with Access Lists

Overview

Standard and extended Cisco IOS access control lists (ACLs) are used to classify IP packets. You can apply a number of features, such as access control (security), encryption, policy-based routing, quality of service (QoS), Network Address Translation (NAT) and port address translation (PAT), to the classified packets. You can also configure standard and extended Cisco IOS access lists on router and switch interfaces. Cisco IOS features are applied on interfaces for specific directions (inbound versus outbound). However, some features use ACLs globally. This module describes the operation of different types of access lists, and shows you how to configure IP access lists.

Upon completing this module, you will be able to:

- Use Cisco IOS commands to configure standard and extended IP access lists, and NAT/PAT, given a functioning router
- Use **show** commands to identify anomalies in standard and extended IP access lists, given an operational router

Outline

The module contains these lessons:

- Access Lists and Their Applications
- Configuring IP Access Lists
- Scaling the Network with NAT and PAT
- Lesson Assessments

Access Lists and Their Applications

Overview

Access control lists (ACLs) provide an important network security feature. With access lists, you can classify packets on inbound and/or outbound routed interfaces. This lesson describes some of the applications for access lists on Cisco Systems networks, and explains how Cisco IOS software processes access lists.

Relevance

By understanding the uses of access lists, you can determine how to implement them on your Cisco network.

Objectives

Upon completing this lesson, you will be able to:

- Explain the purpose of access lists and identify potential applications
- Describe how Cisco IOS software processes standard and extended access lists on inbound and outbound interfaces

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

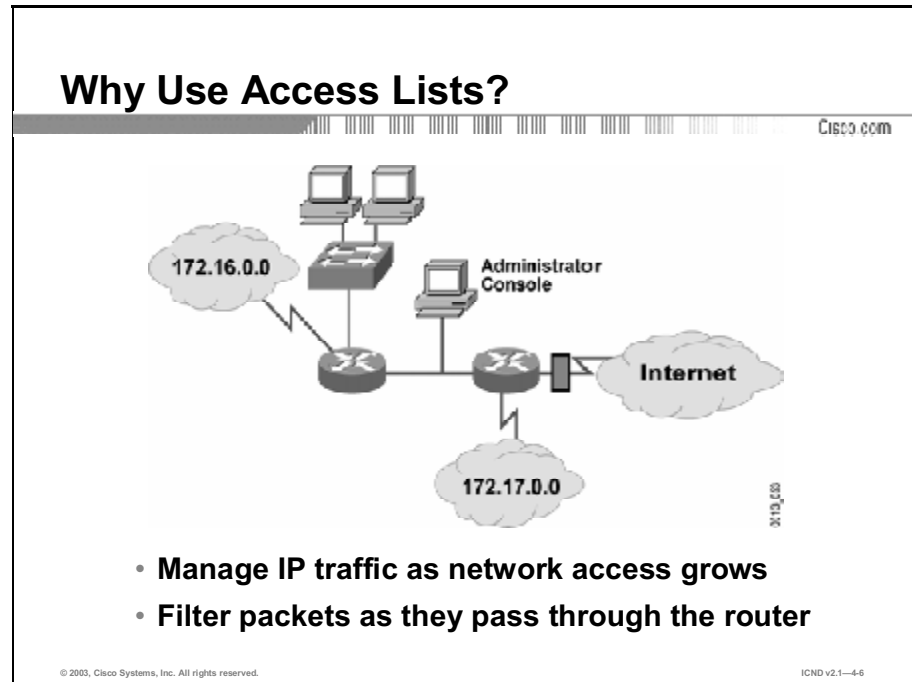
Outline

The lesson includes these topics:

- Overview
- Introducing Access Lists
- Access List Applications
- Types of Access Lists
- How Access Lists Operate
- Testing Against Access List Statements
- Wildcard Masking
- Summary
- Quiz

Introducing Access Lists

Access lists are lists that are kept by routers to identify particular traffic. One application of access lists is to filter traffic into or out of a router interface. Access lists also manage IP traffic as network access grows. This topic illustrates the need for access lists.



The earliest routed networks connected a modest number of LANs and hosts. As router connections increase to legacy and outside networks, and with the increased use of the Internet, there will be new challenges to control access. Network administrators face the dilemma of how to deny unwanted traffic while allowing appropriate access. Although other tools such as passwords, callback equipment, and physical security devices are helpful, they often lack the flexible and specific controls that most administrators prefer.

Access lists offer an important tool for controlling traffic on the network. These lists allow you to filter the packet flow into or out of router interfaces to help limit network traffic and restrict network use by certain users or devices.

Example of Access List Implementation

The figure illustrates the main reason a network administrator would employ access lists. The network originally includes a single Ethernet segment. The workstation represents the administrator console to the router.

As the network grows, the administrator now has to deal with traffic from multiple networks, devices, and from the Internet. In order to filter the extensive traffic and secure the networks, the administrator can implement access lists.

Access List Applications

An IP access list is a sequential list of permit and deny conditions that apply to IP addresses or upper-layer IP protocols. Access lists filter traffic going through the router, but they do not filter traffic originating from the router. This topic describes applications for access lists on Cisco Systems networks.

Access List Applications

Cisco.com

Transmission of Packets on an Interface

Virtual Terminal Line Access (IP)

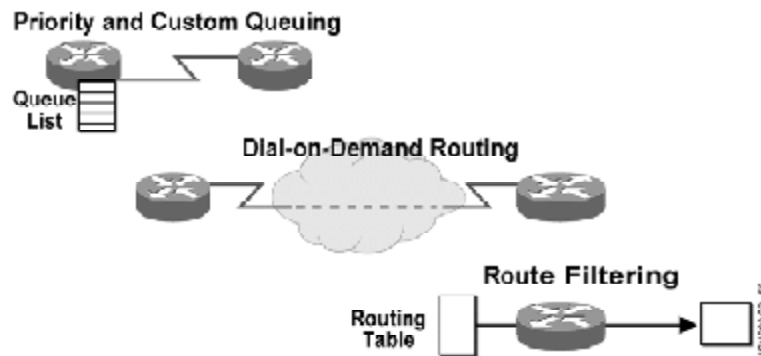
- Permit or deny packets moving through the router.
- Permit or deny vty access to or from the router.
- Without access lists, all packets could be transmitted onto all parts of your network.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—4-7

Packet filtering helps control packet movement through the network. Cisco provides access lists to permit or deny crossing of packets to or from specified router interfaces. Access lists can also be applied to the vty ports of the router to permit or deny Telnet traffic into or out of the router vty ports.

Other Access List Uses

Cisco.com



- **Special handling for traffic based on packet tests**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-8

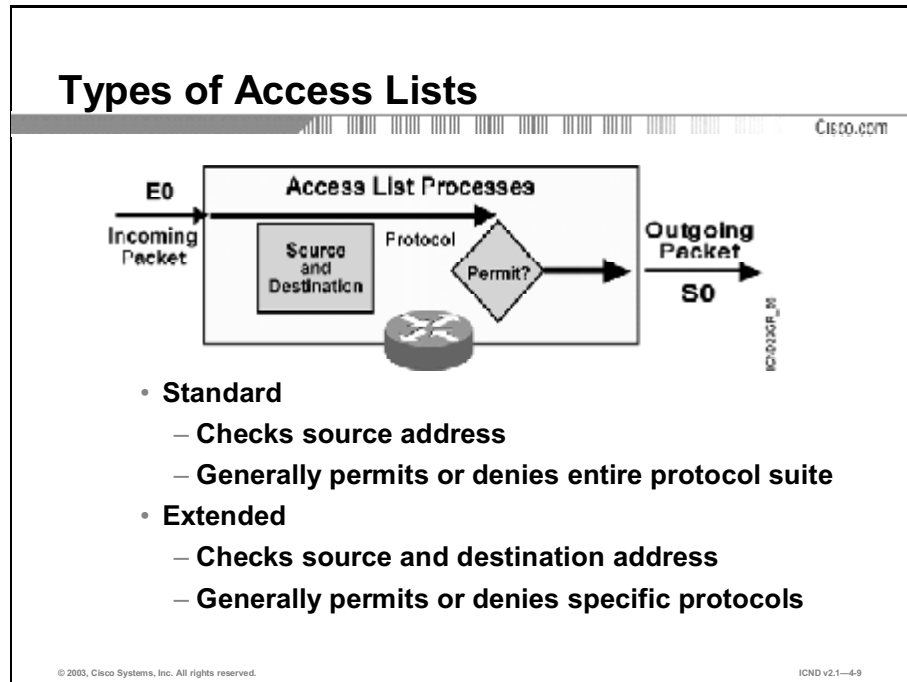
You can also use IP access lists to classify and differentiate traffic so that you can assign different traffic types to different software output queues when there is congestion. This is a useful feature to support different quality of service (QoS) requirements for different traffic. Priority and custom queuing are two of the queuing techniques available in Cisco IOS.

You can also use an access list to identify “interesting” traffic, for example, triggering dial-on-demand routing (DDR).

You can also use access lists for filtering routing protocol updates to or from the router.

Types of Access Lists

Access lists are optional mechanisms in Cisco IOS software that you can configure to filter or test packets to determine whether to forward them to their destination or discard them. This topic illustrates the types of access lists.



There are two general types of access lists, as follows:

- **Standard access lists:** Standard access lists for IP check the source addresses of packets that could be routed. The result permits or denies output for an entire protocol suite, based on the source network, subnet, or host IP address.
- **Extended access lists:** Extended IP access lists check both source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, allowing administrators more flexibility and control.

Access lists express the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router. Access lists do not act on packets that originate from the router itself. Instead, access lists are statements that specify conditions on how the router will handle the traffic flow through specified interfaces.

How to Identify Access Lists

Cisco.com

Access List Type		Number Range/Identifier
IP	Standard	1-99, 1300-1999
	Extended	100-199, 2000-2699
	Named	Name

- **Standard IP lists (1-99) test conditions of all IP packets from source addresses.**
- **Extended IP lists (100-199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports.**
- **Standard IP lists (1300-1999) (expanded range).**
- **Extended IP lists (2000-2699) (expanded range).**
- **Other access list number ranges test conditions for other networking protocols.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-10

Access lists can control most protocols on a Cisco router. The figure shows the number ranges of the access list types for IP.

An administrator enters an access list number as the first argument of the global access list statement. The router identifies which access list software to use based on this numbered entry. Access list statements contain test conditions. These test conditions specify tests according to the rules of the given protocol suite. The test conditions for an access list vary by protocol.

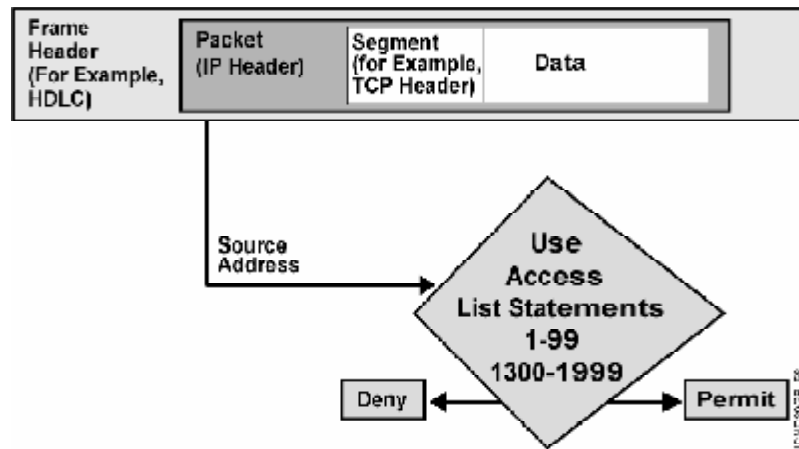
Many access lists are possible for a protocol. Select a different access list number for a given protocol for each new access list. However, you can specify only one access list per protocol, per direction, per interface.

Specifying an access list number from 1 to 99 or 1300 to 1999 instructs the router to accept standard IP access list statements. Specifying an access list number from 100 to 199 or 2000 to 2699 instructs the router to accept extended IP access list statements.

The named access list feature allows you to identify IP standard and extended access lists with an alphanumeric string (name) instead of the numeric representations. Named IP access lists allow you to delete—but not insert—individual entries in a specific access list.

Testing Packets with Standard Access Lists

Cisco.com



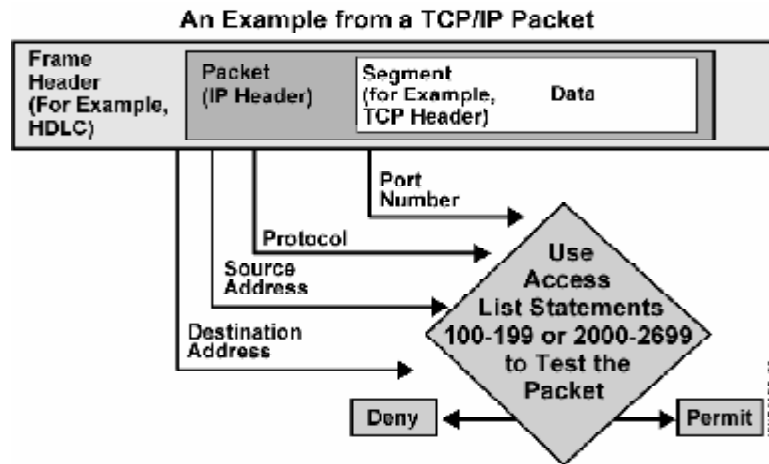
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-11

The standard access list (numbered 1 to 99 and 1300 to 1999) may not provide the traffic filtering control that you need. Standard access lists filter based on a source address and mask, and permit or deny the entire TCP/IP protocol suite. You may need a more precise way to filter your network traffic.

Testing Packets with Extended Access Lists

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-12

For more precise traffic-filtering control, use extended IP access lists, which check for the source and destination address. In addition, at the end of the extended access list statement, you can specify the protocol and optional TCP or User Datagram Protocol (UDP) port number to filter more precisely.

Port numbers can be well-known port numbers. A few of the most common port numbers are shown in the table.

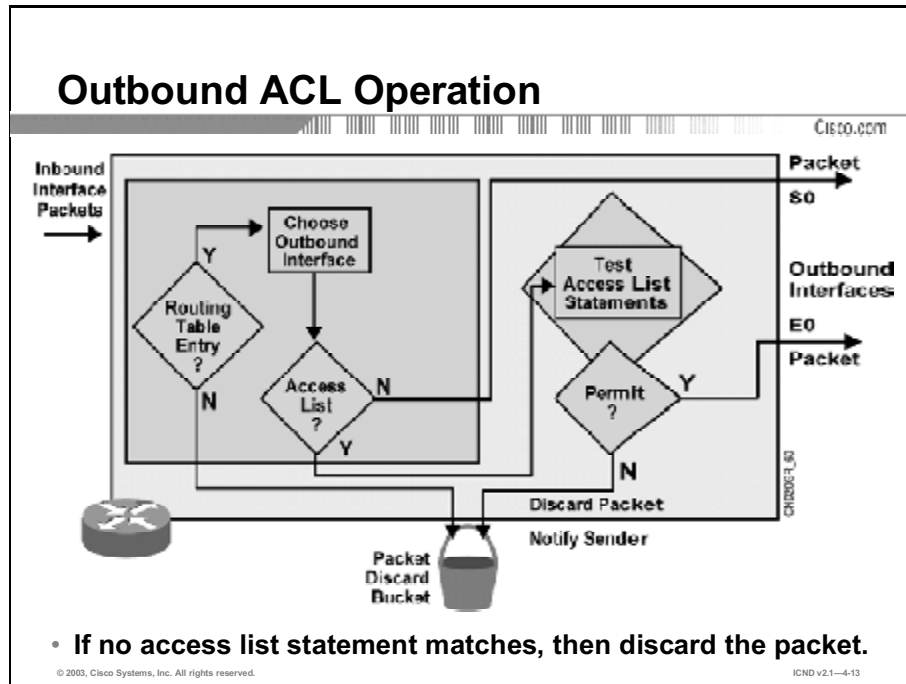
Well-Known Port Number (Decimal)	IP Protocol
20 (TCP)	File Transfer Protocol FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	SMTP ¹
53 (TCP/UDP)	DNS ²
69 (UDP)	TFTP
80 (TCP)	HTTP

¹SMTP = Simple Mail Transfer Protocol

²DNS = Domain Name System

How Access Lists Operate

Inbound access lists process incoming packets before they are routed to an outbound interface, while outbound access lists process packets to an outbound interface. This topic explains how access lists operate.



Access control lists (ACLs) express the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router. Access lists do not act on packets that originate from the router itself. Instead, access lists are statements that specify conditions on how the router will handle the traffic flow through specified interfaces.

You can apply access lists as follows:

- **Inbound access lists:** Incoming packets are processed before being routed to an outbound interface. An input access list is efficient because it saves the overhead of routing lookups if the packet is to be discarded after being denied by the filtering tests. If the packet is permitted by the tests, it is then processed for routing.
- **Outbound access lists:** Incoming packets are routed to the outbound interface and then processed through the outbound access list.

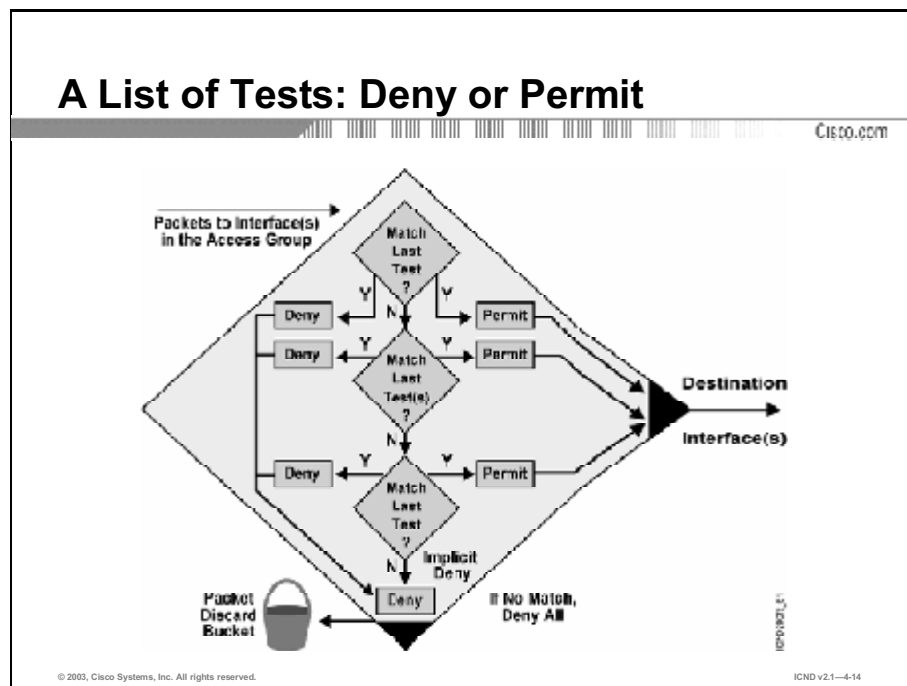
The figure shows an example of an outbound access list. The beginning of the process is the same, regardless of whether outbound access lists are used. When a packet enters an interface, the router checks to see whether it is routable by checking the routing table. If the packet is not routable, the packet will be dropped.

Next, the router checks to see whether the destination interface is grouped to an access list. If not, the packet can be sent to the output buffer. The following are examples:

- If the outbound interface is S0, which has not been grouped to an outbound access list, the packet is sent to S0 directly.
- If the outbound interface is E0, which has been grouped to an outbound access list, before the packet can be sent out on E0, it is tested by the combination of access list statements associated with that interface. Based on the access list tests, the packet will be permitted or denied.
- For outbound lists, *to permit* means to send it to the output buffer, and *to deny* means to discard the packet. For inbound lists, *to permit* means to continue to process the packet after receiving it on an inbound interface, and *to deny* means to discard the packet. When discarding packets, some protocols return a special packet to notify the sender that the destination is unreachable. For the IP protocol, an ACL discard will result in a “Destination unreachable (U.U.U)” response to a ping, and an “Administratively prohibited (!A * !A)” response to a traceroute.

Testing Against Access List Statements

Cisco IOS software executes access list statements in sequential order, so the first statement is processed, then the next, and so on. This topic explains how Cisco IOS software processes access list statements.



Access list statements operate in sequential, logical order. They evaluate packets from the top down, one statement at a time. If a packet header and an access list statement match, the rest of the statements in the list are skipped and the packet is permitted or denied as determined by the matched statement. If a packet header does not match an access list statement, the packet will then be tested against the next statement in the list. This matching process continues until the end of the list is reached.

A final implied statement covers all packets for which conditions did not test true. This final test condition matches all other packets and results in a “deny” instruction. Instead of proceeding into or out of an interface, all these remaining packets are dropped. This final statement is often referred to as the “implicit deny any” statement. Because of the implicit deny any statement, an access list should have at least one permit statement in it; otherwise, the access list will block all traffic.

You can apply an access list to multiple interfaces. However, there can be only one access list per protocol, per direction, per interface.

Wildcard Masking

Address filtering occurs when you use access list address wildcard masking to identify how to check or ignore corresponding IP address bits. This topic describes how wildcard masking is used with access lists.

Wildcard Bits: How to Check the Corresponding Address Bits

Cisco.com

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	= Check All Address Bits (Match All)
0	0	1	1	1	1	1	1	= Ignore Last 6 Address Bits
0	0	0	0	1	1	1	1	= Ignore Last 4 Address Bits
1	1	1	1	1	1	0	0	= Check Last 2 Address Bits
1	1	1	1	1	1	1	1	= Do Not Check Address (Ignore Bits in Octet)

Octet Bit Position and Address Value for Bit

Examples

- 0 means check value of corresponding address bit.
- 1 means ignore value of corresponding address bit.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—4-15

Wildcard masking for IP address bits uses the number 1 and the number 0 to identify how to treat the corresponding IP address bits, as follows:

- A wildcard mask bit 0 means “check the corresponding bit value” in the address.
- A wildcard mask bit 1 means “do not check (ignore) that corresponding bit value” in the address.

This type of mask is sometimes referred to as an “inverted mask.”

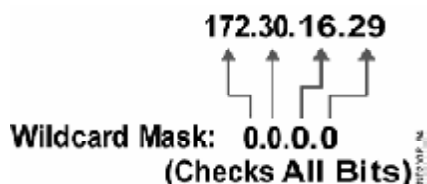
By carefully setting wildcard masks, an administrator can select single or several IP addresses for permit or deny tests with one access list statement. Refer to the example in the figure.

Note Wildcard masking for access lists operates differently from an IP subnet mask. A 0 in a bit position of the access list mask indicates that the corresponding bit in the address must be checked; a 1 in a bit position of the access list mask indicates the corresponding bit in the address is not “interesting” and can be ignored.

Wildcard Bits to Match a Specific IP Host Address

Cisco.com

- Check all the address bits (match all).
 - Verify an IP host address, for example:



- For example, **172.30.16.29 0.0.0.0** checks all the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword **host** (**host 172.30.16.29**).

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-16

You have seen how the 0 and 1 bits in an access list wildcard mask cause the access list to either *check* or *ignore* the corresponding bit in the IP address. The figure shows an example of how the wildcard masking process is applied.

Consider a network administrator who wants to specify that a specific IP host address will be denied in an access list test. To indicate a host IP address, the administrator would enter the full address, for example, 172.30.16.29. Then, to indicate that the access list should check all the bits in the address, the corresponding wildcard mask bits for this address would be all 0s, that is, 0.0.0.0 in dotted-decimal-notation.

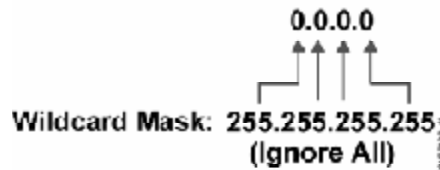
Working with decimal representations of binary wildcard mask bits can be tedious. For the most common uses of wildcard masking, you can use abbreviations. These abbreviation words reduce how many numbers you are required to enter while configuring address test conditions. One example where you can use an abbreviation instead of a long wildcard mask string is when you want to match a host address.

You can use the abbreviation **host** to communicate this same test condition to Cisco IOS access list software. In the example, instead of entering **172.30.16.29 0.0.0.0**, the administrator can use the string **host 172.30.16.29**.

Wildcard Bits to Match Any IP Address

Cisco.com

- **Test conditions: Ignore all the address bits (match any).**
 - **An IP host address, for example:**



- **Accept any address: any**
- **Abbreviate the expression using the keyword any.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-17

A second common condition where Cisco IOS software will permit an abbreviation term in the access list wildcard mask is when you want to match all the bits of any IP address.

Consider a network administrator who wants to specify that any address will be permitted in an access list test. To indicate any IP address, the administrator would enter the IP address of 0.0.0.0. Then, to indicate that the access list should ignore (allow without checking) any bit value within the IP address, the corresponding wildcard mask bits for this address would be all ones (255.255.255.255).

You can use the abbreviation **any** to communicate this same test condition to Cisco IOS access list software. In the example, instead of entering **0.0.0.0 255.255.255.255**, you can use the word **any** by itself as the keyword.

Wildcard Bits to Match IP Subnets

Cisco.com

- Check for IP subnets 172.30.16.0/24 to 172.30.31.0/24.

- Address and wildcard mask:

172.30.16.0 0.0.15.255

Network .Host	
172.30.16.0	
	0 0 0 1 0 0 0 0
Wildcard Mask:	0 0 0 0 1 1 1 1
	<--- Match ---> <--- Don't Care --->
	0 0 0 1 0 0 0 0 = 16
	0 0 0 1 0 0 0 1 = 17
	0 0 0 1 0 0 1 0 = 18
	⋮
	0 0 0 1 1 1 1 1 = 31

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-18

In the figure, an administrator wants to test a range of IP subnets that will be permitted or denied. Assume the IP address is a class B address (the first two octets are the network number) with eight bits of subnetting (the third octet is for subnets). The administrator wants to use the IP wildcard masking bits to match subnets 172.30.16.0/24 to 172.30.31.0/24.

To use one access list statement to match this range of subnets, the IP address to be used in the access list will be 172.30.16.0 (the first subnet to be matched) followed by the required wildcard mask.

First, the wildcard mask will check the first two octets (172.30) of the IP address using corresponding 0 bits in the first two octets of the wildcard mask.

Because there is no interest in an individual host, the wildcard mask will ignore the final octet by using corresponding one bit in the wildcard mask. (The final octet of the wildcard mask is 255 in decimal, for example.)

In the third octet, where the subnet address occurs, the wildcard mask of decimal 15, or binary 00001111, will match the high order four bits of the IP address. In this case, it will match subnets starting with the 172.30.16.0/24 subnet. For the final (low-end) four bits in this octet, the wildcard mask will indicate that the bits can be ignored. In these positions, the address value can be binary 0 or binary 1. Thus, the wildcard mask matches subnet 16, 17, 18, and so on up to subnet 31. The wildcard mask will not match any other subnets.

In this example, the address 172.30.16.0 with the wildcard mask 0.0.15.255 matches subnets 172.30.16.0/24 to 172.30.31.0/24.

In some cases, you must use more than one access list statement to match a range of subnets; for example, to match 10.1.4.0/24 to 10.1.8.0/24, use 10.1.4.0 0.0.3.255 and 10.1.8.0 0.0.0.255.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Access lists offer a powerful tool for network control.** These lists add the flexibility to filter the packet flow into or out of router interfaces. Such control can help limit network traffic and restrict network use by certain users or devices.
- **An IP access list is a sequential list of permit and deny conditions that apply to IP addresses or upper-layer IP protocols.** Access lists filter traffic going through the router, but they do not filter traffic originated from the router.
- **Access lists are optional mechanisms in Cisco IOS software that you can configure to filter or test packets to determine whether to forward them to their destination or discard them.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-19

Summary (Cont.)

Cisco.com

- **Inbound access lists process incoming packets before they are routed to an outbound interface, while outbound access lists process packets to an outbound interface.**
- **The Cisco IOS software executes access list statements in sequential order, so the first statement is processed, then the next, and so on.**
- **Address filtering occurs using access list address wildcard masking to identify how to check or ignore corresponding IP address bits.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-20

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) What type of dilemma do network administrators face as the network grows to provide appropriate network access?
- A) how to prevent network users from accessing Internet sites
 - B) how to keep customers from accessing the internal network
 - C) how to prevent users from accessing the network from the Internet
 - D) how to deny unwanted connections while allowing appropriate access
- Q2) What is one major benefit that access control lists (ACLs) provide to network administrators over other tools?
- A) callback ability
 - B) physical security
 - C) flexible and specific control
 - D) authenticated network access
- Q3) Which two statements best describe the functionality provided by an access list on a Cisco router? (Choose two.)
- A) An access list filters traffic going through the router.
 - B) An access list filters traffic originating from the router.
 - C) An access list contains only a single permit or deny condition.
 - D) An access list is a sequential list of permit and deny conditions.
 - E) An access list filters all traffic going through the router and originating from the router.
- Q4) Access lists can be applied to vty ports to permit or deny _____ into or out of the router vty ports.
- A) all traffic
 - B) data packets
 - C) Telnet traffic
 - D) all IP packets
- Q5) What are the two basic types of access lists? (Choose two.)
- A) global access lists
 - B) standard access lists
 - C) extended access lists
 - D) privileged access lists
 - E) controlled access lists

- Q6) Which statement describes the drawback of using standard IP access lists?
- A) IP standard access lists permit or deny the entire TCP/IP protocol suite only.
 - B) IP standard access lists check for source address and destination address only.
 - C) IP standard access lists allow you to check only for specific TCP or UDP ports.
 - D) IP standard access lists provide precise traffic-filtering control, but are difficult to configure.
- Q7) What does a Cisco router do with a packet when it encounters an outbound access list permit statement?
- A) It discards the packet.
 - B) It returns the packet to its originator.
 - C) It sends the packet to the output buffer.
 - D) It holds the packet for further processing.
- Q8) Match each step that a Cisco router goes through to process an outbound access list to its description.
- _____ 1. Step 1
 - _____ 2. Step 2
 - _____ 3. Step 3
- A) Permit or deny the packet.
 - B) Check the routing table for routability.
 - C) Check the destination interface assignment to an access list.
- Q9) A packet is entering a Cisco router and is being checked by an access list. What does the router do if the packet does not match any statement in the access list?
- A) The router drops the packet.
 - B) The router routes the packet normally.
 - C) The router creates an alarm, and then routes the packet normally.
 - D) The router creates a log entry and then routes the packet normally.
- Q10) Because of the implicit deny any, an access list must have _____ in it. Otherwise, the access list will block all traffic.
- A) one allow all
 - B) one implicitly permit any
 - C) at least one deny statement
 - D) at least one permit statement

- Q11) What does it mean when an access list wildcard mask bit is set to zero on a Cisco router?
- A) The address is a network or subnet address.
 - B) The router checks the corresponding bit in the address.
 - C) The router ignores the corresponding bit in the address.
 - D) The corresponding bit in the address is in the host field.
- Q12) An administrator on a Cisco router wants to use one access list statement to permit a range of IP subnets. The IP subnets are 10.0.4.0/24 through 10.0.7.0/24. Which address and wildcard mask should the administrator use?
- A) 10.0.4.0 0.0.3.255
 - B) 10.0.4.0 0.0.4.255
 - C) 10.0.7.0 0.0.255.255
 - D) 10.0.7.0 0.0.31.255

Quiz Answer Key

- Q1) D
Relates to: Introducing Access Lists
- Q2) C
Relates to: Introducing Access Lists
- Q3) A, D
Relates to: Access List Applications
- Q4) C
Relates to: Access List Applications
- Q5) B, C
Relates to: Types of Access Lists
- Q6) A
Relates to: Types of Access Lists
- Q7) C
Relates to: How Access Lists Operate
- Q8) 1-B, 2-C, 3-A
Relates to: How Access Lists Operate
- Q9) A
Relates to: Testing Against Access List Statements
- Q10) D
Relates to: Testing Against Access List Statements
- Q11) B
Relates to: Wildcard Masking
- Q12) A
Relates to: Wildcard Masking

Configuring IP Access Lists

Overview

Cisco Systems IOS standard and extended access control lists (ACLs) are used to classify packets. You can subject classified packets to a number of features, such as access control (security), encryption, policy-based routing, and so on. You can also configure standard and extended Cisco IOS access lists on router interfaces and apply them to routed packets. This lesson shows you how to configure, verify, and troubleshoot IP standard and extended access lists.

Relevance

Controlling traffic to certain networks, hosts, and servers is an important component of overall network security. After you configure switching and routing, you should configure access lists.

Objectives

Upon completing this lesson, you will be able to:

- Use Cisco IOS commands to configure IP standard and extended access lists, given a functioning router
- Use **show** commands to identify anomalies in IP standard and extended access lists, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

Outline

The lesson includes these topics:

- Overview
- Implementing Access Lists
- Configuring Standard IP Access Lists
- Configuring Extended IP Access Lists
- Using Named Access Lists
- Configuring Virtual Terminal Access Lists
- Guidelines for Placing Access Lists
- Verifying the Access List Configuration
- Summary
- Quiz

Implementing Access Lists

Well-designed and well-implemented access lists will add an important security component to your network. This topic provides some general guidelines to help you implement access lists.

Access List Configuration Guidelines



- **Access list numbers indicate which protocol is filtered.**
- **One access list per interface, per protocol, per direction is allowed.**
- **The order of access list statements controls testing.**
- **Place the most restrictive statements at the top of list.**
- **There is an implicit deny any statement as the last access list test. Every list needs at least one permit statement.**
- **Create access lists before applying them to interfaces.**
- **Access lists filter traffic going through the router; they do not apply to traffic originating from the router.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—4.4

Follow these general principles to ensure that the access lists you create have the intended results:

- Use numbers from the assigned range only for the protocol and type of list you are creating.
- Only one access list per protocol, per direction, per interface is allowed. Multiple access lists are permitted per interface, but each must be for a different protocol.
- Your access list should be organized to allow top-down processing.
 - Organize your access list so that more specific references in a network or subnet appear before more general ones. Place conditions that occur more frequently before conditions that occur less frequently.
 - Subsequent additions are always added to the end of the access list.
 - You cannot selectively add or remove lines when using numbered access lists, but you can when using named IP access lists. With named IP access lists, additions are still added to the end of the access list.
- Your access list must contain an implicit deny all statement at the end.
 - Unless you end your access list with an explicit permit any statement, by default it will deny all traffic that fails to match any of the access list lines.
 - Every access list should have at least one permit statement. Otherwise, all traffic will be denied.
- You must create the access list before applying it to an interface. An interface with an empty access list applied to it permits all traffic.
- Access lists filter only traffic going through the router. They do not filter traffic originating from the router.

Access List Command Overview

Cisco.com

Step 1: Set parameters for this access list test statement (which can be one of several statements).

```
Router(config)#access-list access-list-number
{permit | deny} {test conditions}
```

Step 2: Enable an interface to use the specified access list.

```
Router(config-if)#{protocol} access-group
access-list-number {in | out}
```

- **Standard IP lists (1-99)**
- **Extended IP lists (100-199)**
- **Standard IP lists (1300-1999) (expanded range)**
- **Extended IP lists (2000-2699) (expanded range)**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-5

In practice, access list commands can be lengthy character strings. Access lists can be complicated to enter or interpret. However, you can simplify the understanding of general access list configuration commands by reducing the commands to two general elements, as indicated by Steps 1 and 2 in the figure:

Step 1 Set parameters for the access list test statements.

Step 2 Enable an interface to use the specified access list.

The access list contains global statements, as follows:

- A global statement identifies the access list, usually an access list number. This number refers to the type of access list that is permitted. Access lists for IP may also use an access list name rather than a number.
- The permit or deny term in the global access list statement indicates how packets that meet the test conditions will be handled by Cisco IOS software. Permit usually means the packet will be allowed to use one or more interfaces that you will specify later. Deny usually means to discard the packet.
- The final term or terms specify the test conditions used by this access list statement. The test can be as simple as checking for a single source address. Usually, test conditions are extended to include several test conditions. Use several global access list statements with the same access list number or name to stack several test conditions into a logical sequence or list of tests.

Use the **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} interface configuration command to activate an IP access list on an interface. The **in** option filters on inbound packets, while the **out** option filters on outbound packets.

Note If you apply an access list with the **ip access-group** command to an interface before you create any access list lines, the result will be “permit any.” The list is “live,” so if you enter only one line, it changes from a permit any to a “deny most” (because of the implicit “deny all” at the end) as soon as you press **Return**. For this reason, create your access list before you apply it to an interface.

Note You can apply one access list per protocol, per interface, per direction.

Configuring Standard IP Access Lists

To configure standard IP access lists on a Cisco router, you will create a standard IP access list and activate an access list on an interface. This topic explains how to create and activate a standard IP access list.

Standard IP Access List Configuration

CISCO.COM

```
Router(config)#access-list access-list-number
{permit | deny | remark} source [mask]
```

- Sets parameters for this list entry
- IP standard access lists use 1 to 99
- Default wildcard mask = 0.0.0.0
- no access-list *access-list-number* removes entire access list
- remark option lets you add a description for the access list

```
Router(config-if)#ip access-group
access-list-number {in | out}
```

- Activates the list on an interface
- Sets inbound or outbound testing
- Default = outbound
- no ip access-group *access-list-number* removes access list from the interface

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-6

The procedure outlined in the table describes how to configure standard access lists on a router.

Step	Action	Notes
1.	Create an entry in a standard IP traffic filter list using the access-list global configuration command. Router(config)# access-list 1 172.16.0.0 0.0.255.255	Enter the global no access-list access-list-number command to remove the entire access list. The example statement matches any address that starts with 172.16.x.x. Use the remark option to add a description to your access list.
2.	Select an interface to enable the access list using the interface configuration command. Router(config)# interface ethernet 1	After you enter the interface command, the CLI ¹ prompt will change from (config) # to (config-if) #.
3.	Activate the existing access list to an interface using the ip access-group interface configuration command. Router(config-if)# ip access-group 1 out	To remove an IP access list from an interface, enter the no ip access-group access-list-number command on the interface.

¹CLI = command-line interface

The **access-list** command creates an entry in a standard IP traffic filter list.

access-list Command Parameters	Description
<i>access-list-number</i>	Identifies the list to which the entry belongs; a number from 1 to 99.
permit deny	Indicates whether this entry allows or blocks traffic from the specified address.
<i>source</i>	Identifies the source IP address.
<i>source-mask</i>	Identifies which bits in the address field are matched. The default mask is 0.0.0.0. (Match all bits.)

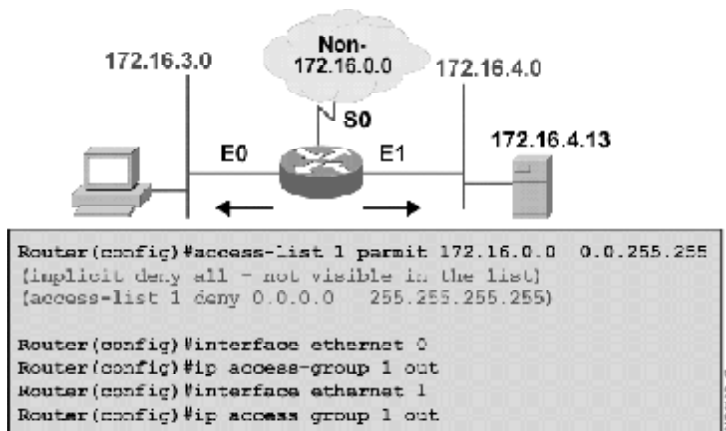
The **ip access-group** command links an existing access list to an interface. Only one access list per protocol, per direction, per interface is allowed.

ip access-group Command Parameters	Description
<i>access-list-number</i>	Indicates the number of the access list to be linked to this interface.
in out	Selects whether the access list is applied as an incoming or outgoing filter; if in or out is not specified, out is the default.

Note	To remove an IP access list from an interface, first enter the no ip access-group command on the interface; then enter the global no access-list command to remove the entire access list.

Standard IP Access List Example 1

Cisco.com



- **Permit my network only.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-7

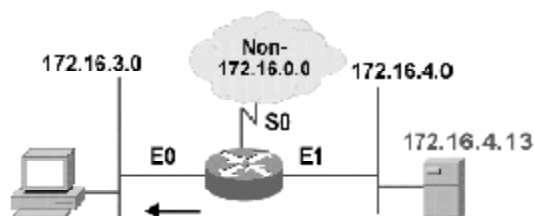
The table describes the access list presented in the figure.

access-list Command Parameters	Description
1	Access list number that indicates this is a standard list.
permit	Traffic that matches selected parameters will be forwarded.
172.16.0.0	IP address that will be used with the wildcard mask to identify the source network.
0.0.255.255	Wildcard mask; 0s indicate positions that must match; 1s indicate "don't care" positions.
ip access-group 1 out	Links the access list to the interface as an outbound filter.

This access list allows only traffic from source network 172.16.0.0 to be forwarded out on E0 and E1. Traffic from networks other than 172.16.0.0 is blocked.

Standard IP Access List Example 2

Cisco.com



```
Router(config)#access-list 1 deny 172.16.4.13 0.0.0.0
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

Router(config)#interface ethernet 0
Router(config)#ip access-group 1 out
```

- Deny a specific host.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-8

The tables describe the access lists in the examples.

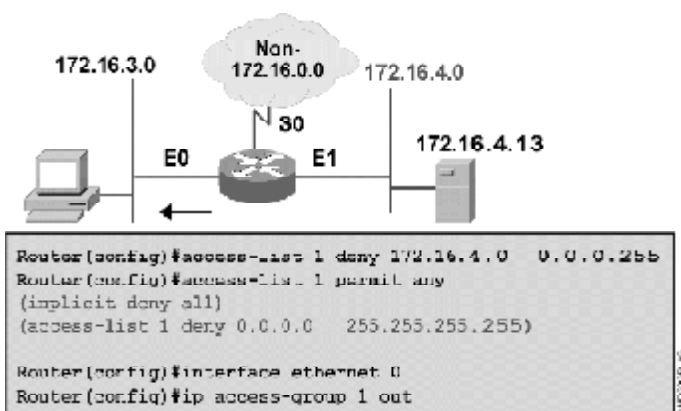
access-list Command Parameters	Description
1	Access list number that indicates this is a standard list.
deny	Traffic that matches selected parameters will not be forwarded.
172.16.4.13	IP address of the source host.
0.0.0.0	This mask requires the test to match all bits. (This is the default mask.)

access-list Command Parameters	Description
1	Access list number that indicates this is a standard list.
permit	Traffic that matches selected parameters will be forwarded.
0.0.0.0	IP address of the source host; all 0s indicate a placeholder.
255.255.255.255	Wildcard mask; 0s indicate positions that must match, 1s indicate "don't care" positions. All 1s in the mask indicate that all 32 bits will <i>not</i> be checked in the source address.

This access list is designed to block traffic from a specific address, 172.16.4.13, and to allow all other traffic to be forwarded on interface Ethernet 0. The 0.0.0.0 255.255.255.255 IP address and wildcard mask combination permits traffic from any source. This combination can also be written using the keyword **any**.

Standard IP Access List Example 3

Cisco.com



- Deny a specific subnet.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-9

The tables describe the access list in the example.

access-list Command Parameters	Description
1	Access list number that indicates this is a standard list.
deny	Traffic that matches selected parameters will not be forwarded.
172.16.4.0	IP address of the source subnet.
0.0.0.255	Wildcard mask; 0s indicate positions that must match, 1s indicate “don’t care” positions. The mask with 0s in the first three octets indicates those positions must match; the 255 in the last octet indicates a “don’t care” condition.

access-list Command Parameters	Description
1	Access list number that indicates this is a standard list.
permit	Traffic that matches selected parameters will be forwarded.
any	Abbreviation for the IP address of the source; all 0s indicate a placeholder and the wildcard mask 255.255.255.255. All 1s in the mask indicate that all 32 bits will <i>not</i> be checked in the source address.

This access list is designed to block traffic from a specific subnet, 172.16.4.0, and to allow all other traffic to be forwarded out E0.

Configuring Extended IP Access Lists

To configure extended IP access lists on a Cisco router, you will create an extended IP access list and activate an access list on an interface. This topic explains how to create and activate an extended IP access list.

Extended IP Access List Configuration

Cisco.com

```
Router(config)#access-list access-list-number
{permit | deny} protocol source source-wildcard [operator
port] destination destination-wildcard [operator port]
[established] [log]
```

- Sets parameters for this list entry

```
Router(config-if)#ip access-group access-list-number {in | out}
```

- Activates the extended list on an interface

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-10

The procedure outlined in the table describes how to configure extended access lists on a router.

Step	Action	Notes
1.	Define an extended IP access list using the access-list global configuration command. Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21	Display the contents of the access list using the show access-lists command. In the example, access-list 101 denies TCP traffic from source 172.16.4.0 using the wildcard 0.0.0.255, to destination 172.16.3.0 using the wildcard 0.0.0.255.
2.	Select a desired interface to be configured using the interface global configuration command. Router(config)# interface ethernet 0	After the interface command is entered, the CLI prompt changes from (config)# to (config-if)#.
3.	Link the extended IP access list to an interface using the ip access-group interface configuration command. Router(config-if)# ip access-group 101 in	Verify if an IP access list is applied to the interface using the show ip interfaces command.

The **access-list** command creates an entry to express a condition statement in a complex filter. The table explains the syntax of the command as shown in the figure.

access-list Command Parameters	Description
<i>access-list-number</i>	Identifies the list using a number in the range 100 to 199 or 2000 to 2699.
permit deny	Indicates whether this entry allows or blocks the specified address.
<i>protocol</i>	IP, TCP, UDP ¹ , ICMP ² , GRE ³ , or IGRP ⁴ .
<i>source and destination</i>	Identifies source and destination IP addresses.
<i>source-wildcard and destination-wildcard</i>	Wildcard mask; 0s indicate positions that must match, 1s indicate "don't care" positions.
<i>operator port</i>	<i>lt</i> (less than), <i>gt</i> (greater than), <i>eq</i> (equal), <i>neq</i> (not equal), and a port number.
established	For inbound TCP only; allows TCP traffic to pass if the packet uses an established connection. (For example, it has acknowledgement [ACK] bits set.)
log	Sends a logging message to the console.

¹UDP = User Datagram Protocol

²ICMP = Internet Control Message Protocol

³GRE = generic routing encapsulation

⁴IGRP =Interior Gateway Routing Protocol

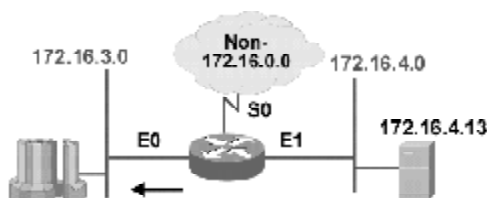
Note The syntax of the **access-list** command presented here is representative of the TCP protocol form. Not all parameters or options are given. For the complete syntax of all forms of the command, refer to the appropriate Cisco IOS software documentation available on CD-ROM or at Cisco.com.

The **ip access-group** command links an existing extended access list to an interface. Only one access list per protocol, per direction, per interface is allowed.

ip access-group Command Parameters	Description
<i>access-list-number</i>	Indicates the number of the access list to be linked to an interface
in out	Selects whether the access list is applied as an input or output filter; if in or out is not specified, out is the default

Extended Access List Example 1

Cisco.com



```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
Router(config)#access-list 101 permit ip any any
Router(config)#interface ethernet 0
Router(config)#ip access-group 101 out
```

- Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0.
- Permit all other traffic.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-11

The table explains the command syntax in the example.

access-list Command Parameters	Description
101	Access list number 101 indicates an extended IP access list.
deny	Traffic that matches selected parameters will be blocked.
tcp	Transport layer protocol.
172.16.4.0 0.0.0.255	Source IP address and mask; the first three octets must match but not the last octet.
172.16.3.0 0.0.0.255	Destination IP address and mask; the first three octets must match but not the last octet.
eq 21	Destination port: specifies the well-known port number for FTP control.
eq 20	Destination port: specifies the well-known port number for FTP data.

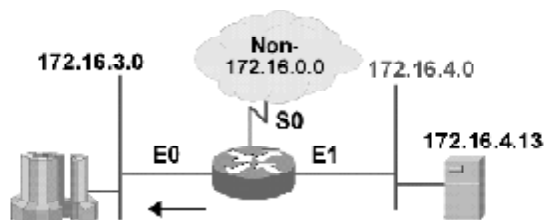
ip access-group 101 Command Parameter	Description
out	Links access list 101 to interface E0 as an output filter

The deny statements deny FTP traffic from subnet 172.16.4.0 to subnet 172.16.3.0.

The permit statement allows all other IP traffic out interface E0.

Extended Access List Example 2

Cisco.com



```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
Router(config)#access-list 101 permit ip any any
{implicit deny all}

Router(config)#interface ethernet 0
Router(config)#ip access-group 101 out
```

- Deny only Telnet from subnet 172.16.4.0 out of E0.
- Permit all other traffic.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-12

The table explains the command syntax in the example.

access-list Command Parameters	Description
101	Access list number; indicates extended IP access list.
deny	Traffic that matches selected parameters will not be forwarded.
tcp	Transport layer protocol.
172.16.4.0 0.0.0.255	Source IP address and mask; the first three octets must match but not the last octet.
any	Match any destination IP address.
eq 23	Destination port: specifies a well-known port number for Telnet.
permit	Traffic that matches selected parameters will be forwarded.
ip	Any IP protocol.
any	Keyword matching traffic from any source.
any	Keyword matching traffic to any destination.

ip access-group 101 Command Parameter	Description
out	Links access list 101 to interface E0 as an output filter

This example denies Telnet traffic from 172.16.4.0 being sent out interface E0. All other IP traffic from any other source to any destination is permitted out E0.

Using Named Access Lists

The named access list feature allows you to identify IP standard and extended access lists with an alphanumeric string (name) instead of the current numeric representations. This topic describes the use of named access lists.

Using Named IP Access Lists

Cisco.com

```
Router(config)#ip access-list {standard | extended} name
```

- **Alphanumeric name string must be unique.**

```
Router(config {std- | ext-}nacl)#{permit | deny}
{ip access list test conditions}
{permit | deny} {ip access list test conditions}
no {permit | deny} {ip access list test conditions}
```

- **Permit or deny statements have no prepended number.**
- **“no” removes the specific test from the named access list.**

```
Router(config-if)#ip access-group name {in | out}
```

- **Activates the IP named access list on an interface.**

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—4-13

With a numbered IP access list, an administrator who wants to alter an access list must first delete the entire numbered access list, and then reconfigure it. An administrator cannot delete individual statements.

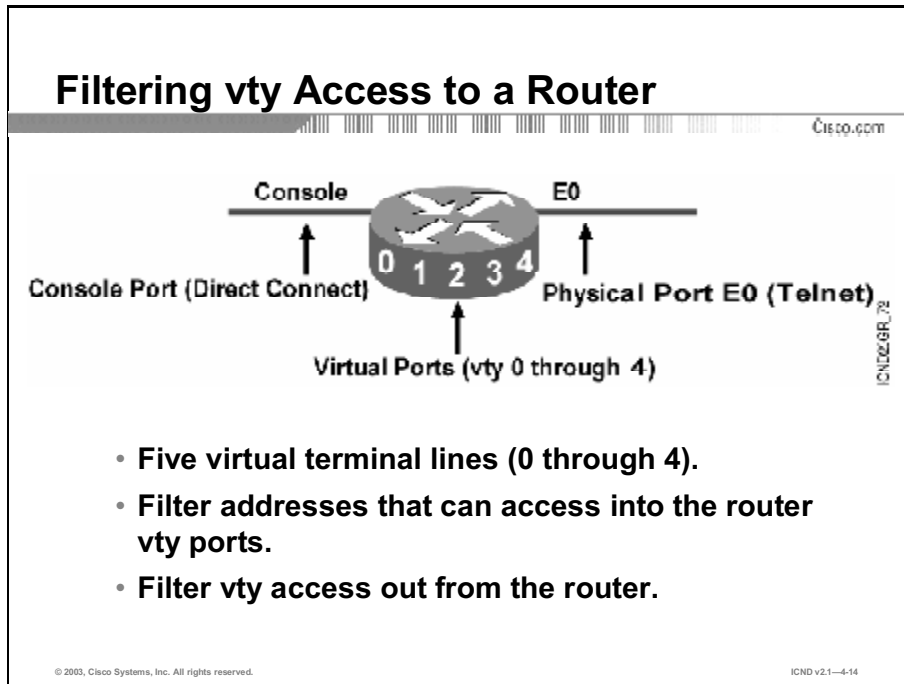
Named IP access lists allow you to delete, but not insert, individual entries in a specific access list. Deleting individual entries enables you to modify your access lists without deleting the entire access list and then reconfiguring it. Use named IP access lists when you want to intuitively identify access lists using an alphanumeric name.

Consider the following before implementing named IP access lists:

- Named IP access lists are not compatible with Cisco IOS releases prior to Release 11.2.
- You cannot use the same name for multiple access lists. In addition, access lists of different types cannot have the same name. For example, you are not permitted to specify a standard access control list named “George” and an extended access control list with the same name.

Configuring Virtual Terminal Access Lists

For security purposes, you can deny vty access to the router, or you can permit vty access to the router but deny Telnet access to destinations from that router. Restricting vty access is primarily a technique for increasing network security. This topic describes the capabilities offered by vty access lists, and shows you how to configure them.

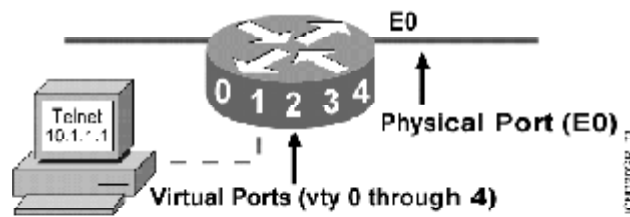


Just as there are physical ports or interfaces such as E0 and E1, there are also virtual ports. A virtual port is called a vty. By default, there are five such virtual terminal lines, numbered vty 0 through vty 4. Some Cisco IOS images can support more than five vty ports.

Standard and extended IP access lists will block packets from going through the router. They are not designed to block packets that originate from the router. By default, an outbound Telnet extended access list does not prevent router-initiated Telnet sessions.

How to Control vty Access

Cisco.com



- Set up an IP address filter with a standard access list statement.
- Use line configuration mode to filter access with the **access-class** command.
- Set identical restrictions on every vty.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-15

Telnet filtering is normally considered an extended IP access list function because it is filtering a higher-level protocol. However, because you will be filtering incoming Telnet sessions by source address and applying filtering to vty lines with the **access-class** command, you can use standard IP access list statements, numbered 1 to 99 and 1300 to 1999.

The **access-class** command also applies standard IP access list filtering to vty lines for outgoing Telnet sessions originating from within the router.

Normally, set identical restrictions on every vty because you cannot control on which vty a user will connect.

Note Some administrators will configure one vty differently from the others. This way they will have a “back door” into the router.

vty Commands

Cisco.com

```
Router(config)#line vty {vty# | vty-range}
```

- **Enters configuration mode for a vty or vty range**

```
Router(config-line)#access-class access-list-number  
{in | out}
```

- **Restricts incoming or outgoing vty connections for address in the access list**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-16

Use the **line** command to place the router in line configuration mode.

line Command Parameters	Description
<code>vty#</code>	Indicates a specific vty line to be configured
<code>vty-range</code>	Indicates a range of vty lines to which the configuration will apply

Use the **access-class** command to link an existing access list to a terminal line or range of lines.

access-class Command Parameters	Description
<code>access-list-number</code>	Indicates the number of the access list to be linked to a terminal line. This is a decimal number from 1 to 99 and 1300 to 2699.
<code>in</code>	Prevents the router from receiving incoming Telnet connections from the addresses in the access list.
<code>out</code>	Prevents the router vty ports from initiating Telnet connections to addresses defined in the standard access list. Note that the source address specified in the standard access list is treated like a destination address when you use access-class out .

vty Access Example

Cisco.com

Controlling Inbound Access

```
access-list 12 permit 192.168.1.0 0.0.0.255
(implicit deny all)
!
line vty 0 4
access-class 12 in
```

- **Permits only hosts in network 192.168.1.0 0.0.0.255 to connect to the router vty**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-17

In this example, we are permitting any device on network 192.168.1.0 0.0.0.255 to establish a virtual terminal (Telnet) session with the router. Of course, the user must know the appropriate passwords to enter user mode and privileged mode.

Notice that identical restrictions have been set on every vty (0 to 4) because you cannot control on which vty a user will connect.

The implicit *deny any statement* still applies to the access list when used as an access class entry.

Guidelines for Placing Access Lists

Access lists can be used to control traffic by filtering and eliminating unwanted packets. Proper placement of an access list can reduce unnecessary traffic on the network. Traffic that will be denied at a remote destination should not use network resources along the route to that destination. This topic provides guidelines to help you determine where to place access lists.

Access List Configuration Principles



- **The order of access list statements is crucial.**
 - **Recommended: Use a text editor on a PC to create the access list statements, then cut and paste them into the router.**
 - **Top-down processing is important.**
 - **Place the more specific test statements first.**
- **No reordering or removal of statements.**
 - **Use the no access-list number command to remove the entire access list.**
 - **Exception: Named access lists permit removal of individual statements.**
- **Implicit deny all will be applied to any packets that do not match any access list statement.**
 - **Unless the access list ends with an explicit permit any statement.**

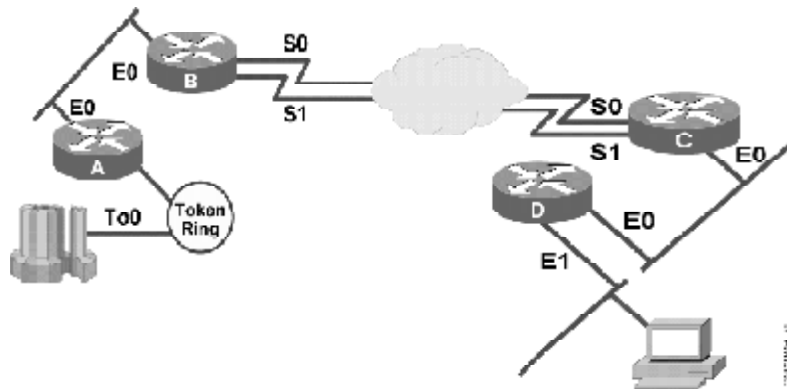
© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—4-18

The following basic principles of access list configuration are given in the figure:

- The order of access list statements is crucial to proper filtering. Cisco recommends that you create the access list using a text editor program on a PC, then cut and paste the access list into the router. For example, you can use Word on a PC to create the access list, then Telnet or console into the router from the PC. Enter the global configuration mode on the router, then cut and paste the access list from the Word document into the router.
- Access lists are processed from the top down. If you place the more specific tests, and tests that will test true frequently, at the beginning of the access list, you can reduce processing overhead.
- Only named access lists allow removal from—but not the reordering of—individual statements from a list. If you want to reorder or remove access list statements, you must remove the whole list and recreate it in the desired order or with the desired statements.
- All access lists end with an implicit deny all statement.

Where to Place IP Access Lists

Cisco.com



- Place extended access lists close to the source.
- Place standard access lists close to the destination.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-19

Suppose an enterprise policy wants to reject Token Ring traffic on router A to the switched Ethernet LAN on E1 port of router D. At the same time, other traffic must be permitted. Several approaches can accomplish this policy.

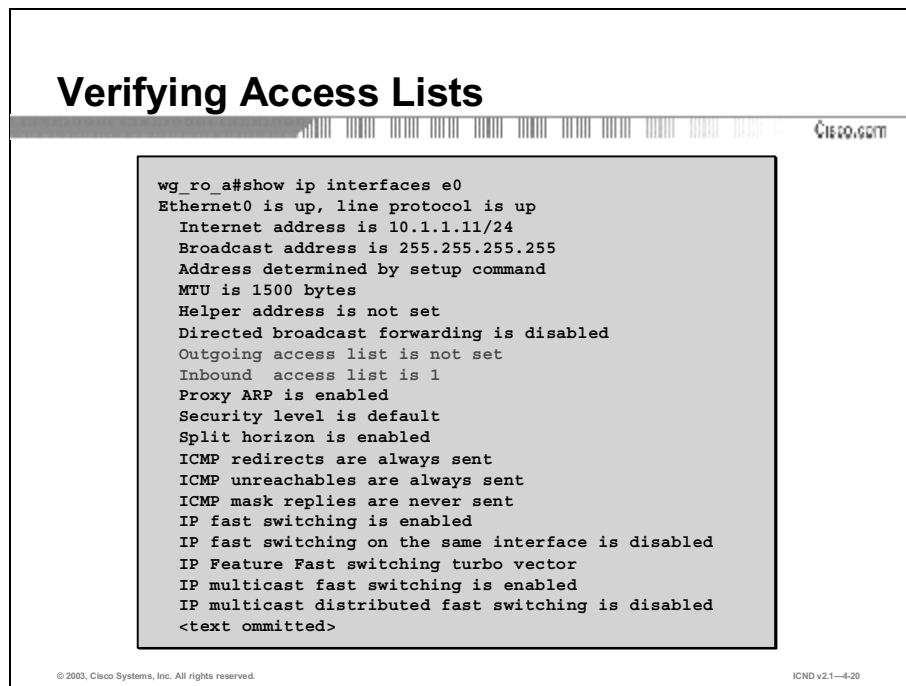
The recommended approach uses an extended access list. It specifies both source and destination addresses. Place this extended access list in router A. Then, packets do not cross router the A Ethernet, do not cross the serial interfaces of routers B and C, and do not enter router D. Traffic with different source and destination addresses can still be permitted.

Extended access lists should normally be placed as close as possible to the source of the traffic to be denied.

Standard access lists do not specify destination addresses. The administrator would have to put the standard access list as near the destination as possible. For example, place an access list on E0 of router D to prevent Token Ring traffic from router A.

Verifying the Access List Configuration

When you finish the access list configuration, you can verify it using the **show** commands. This topic describes the **show** commands that you can use to verify the access list configuration.



Use the **show ip interfaces** command to display IP interface information and indicate whether any IP access lists are set on the interface. In the **show ip interfaces e0** output shown in the figure, IP access list 1 has been configured on the E0 interface as an inbound access list. No outbound IP access list has been configured on the E0 interface.

Monitoring Access List Statements

Cisco.com

```
wg_ro_a#show {protocol} access-list {access-list number}
```

```
wg_ro_a#show access-lists {access-list number}
```

```
wg_ro_a#show access-lists
Standard IP access list 1
  permit 10.2.2.1
  permit 10.3.3.1
  permit 10.4.4.1
  permit 10.5.5.1
Extended IP access list 101
  permit tcp host 10.22.22.1 any eq telnet
  permit tcp host 10.33.33.1 any eq ftp
  permit tcp host 10.44.44.1 any eq ftp-data
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-21

Use the **show access-lists** command to display the contents of all access lists. By entering the access list name or number as an option for this command, you can display a specific access list. To display only the contents of all IP access lists, use the **show ip access-list** command.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Well-designed and implemented access lists will add an important security component to your network.**
- **To configure standard IP access lists on a Cisco router, you will create a standard IP access list and activate an access list on an interface.**
- **Similarly, to configure extended IP access lists on a Cisco router, you will create an extended IP access list range and activate an access list on an interface.**
- **The named access list feature allows you to identify IP standard and extended access lists with an alphanumeric string (name) instead of the current numeric (1 to 199 and 1300 to 2699) representations.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-22

Summary (Cont.)

Cisco.com

- **For security purposes, you can deny Telnet access to the router, or you can permit Telnet access to the router but deny access to destinations from that router. Restricting Telnet access is primarily a technique for increasing network security.**
- **Access lists are used to control traffic by filtering and eliminating unwanted packets. Proper placement of an access list statement can reduce unnecessary traffic.**
- **When you finish the access list configuration, you can verify it using the show commands.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-23

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which statement about access lists is true?
- A) Access lists are processed from the bottom up.
 - B) All access lists end with an implicit “allow all” statement.
 - C) The order of access list statements is crucial to proper filtering.
 - D) Standard access lists allow removal and reordering of individual statements from a list.
- Q2) What does the first global statement in an access list specify?
- A) deny term
 - B) permit term
 - C) access list number
 - D) access list conditions
- Q3) A system administrator wants to configure an IP standard access list statement on a Cisco router to deny only packets from host 10.1.1.7 on the subnet 10.1.1.0/24. Which configuration accomplishes this goal?
- A) access-list 1 deny 10.1.1.7
 - B) access-list 1 deny 10.1.1.7 host
 - C) access-list 27 deny 0.0.0.0 10.1.1.7
 - D) access-list 99 deny 10.1.1.7 255.255.255.0
- Q4) What is the complete command to enable an access list on a router interface with the following parameters?
- IP access list number is 1
 - List will check outbound packets
- A) **ip access-list 1 out**
 - B) **ip access-group 1 in**
 - C) **ip access-group 1 out**
 - D) **ip-access list 1 deny out**

- Q5) What does the **established** keyword in an IP extended access list statement specify?
- A) TCP traffic will match the statement if it is trying to establish a connection (SYN bit set).
 - B) TCP traffic will match the statement if it is part of an already established connection (acknowledgement [ACK] bit set).
 - C) TCP and UDP traffic will match the statement if it is trying to establish a connection (synchronize [SYN] bit set).
 - D) TCP and UDP traffic will match the statement if it is part of an already established connection (ACK bit set).

- Q6) The following is an access list entered on a Cisco router.

```
access-list 130 permit ip 172.16.16.0 0.0.15.255 172.16.32.0 0.0.15.255
```

If this access list is used to control incoming packets on Ethernet 0, which four statements are true? (Choose four.)

- A) Address 172.16.1.1 will be denied access to address 172.16.37.5.
 - B) Address 172.16.1.1 will be permitted access to address 172.16.32.1.
 - C) Address 172.16.16.1 will be permitted access to address 172.16.32.1.
 - D) Address 172.16.31.1 will be permitted access to address 172.16.45.1.
 - E) Address 172.16.16.1 will be permitted access to address 172.16.50.1.
 - F) Address 172.16.30.12 will be permitted access to address 172.16.32.12.
- Q7) Which statement best describes named access lists on a Cisco router?
- A) Named access lists allow you to insert individual lines into an access list.
 - B) Named access lists allow you to delete individual lines from an access list.
 - C) Named access lists allow you to identify access lists using any keyboard character.
 - D) Named access lists allow you to create up to 200 standard access lists, other than the 99 standard access lists.
- Q8) A system administrator has created a five-line access list with the identifier 100 on a Cisco router. There is an error in the third line and this line needs to be replaced. How can the system administrator fix this problem?
- A) The system administrator can delete the third line and then reenter it.
 - B) The system administrator will have to delete all lines in the access list. All lines will then need to be reentered.
 - C) The system administrator can delete each line, starting at the end of the list, until the incorrect line is deleted. The last three lines then need to be reentered.
 - D) The system administrator can delete each line, starting at the beginning of the list, until the incorrect line is deleted. The first three lines then need to be reentered.

- Q9) How many vty lines are there on a Cisco router by default?
- A) 4 vty lines, 0 through 3
 - B) 4 vty lines, 1 through 4
 - C) 5 vty lines, 0 through 4
 - D) 10 vty lines, 1 through 10
- Q10) Which command is used to apply a standard IP access list to a vty port for restricting incoming Telnet access to the router?
- A) **access-list** access-list number **in**
 - B) **access-vty** access-list number **in**
 - C) **access-class** access-list number **in**
 - D) **access-group** access-list number **in**
- Q11) All access lists end with a(n) _____ statement.
- A) deny tcp
 - B) access-list deny
 - C) implicit deny all
 - D) implicit permit all
- Q12) How are access lists processed?
- A) from the top down
 - B) from the bottom up
 - C) beginning at the first deny statement
 - D) beginning at the first permit statement
- Q13) Which command is used on a Cisco router to determine if IP access lists are applied to any interfaces?
- A) **show interfaces**
 - B) **show access lists**
 - C) **show ip interface**
 - D) **show ip access-list**
- Q14) Which command is used to find out if access list 100 has been configured on a Cisco router?
- A) **show interfaces**
 - B) **show ip interface**
 - C) **show ip access-list**
 - D) **show access-groups**

Quiz Answer Key

- Q1) C
Relates to: Implementing Access Lists
- Q2) C
Relates to: Implementing Access Lists
- Q3) A
Relates to: Configuring Standard IP Access Lists
- Q4) C
Relates to: Configuring Standard IP Access Lists
- Q5) B
Relates to: Configuring Extended IP Access Lists
- Q6) A, C, D, F
Relates to: Configuring Extended IP Access Lists
- Q7) B
Relates to: Using Named Access Lists
- Q8) B
Relates to: Using Named Access Lists
- Q9) C
Relates to: Configuring Virtual Terminal Access Lists
- Q10) C
Relates to: Configuring Virtual Terminal Access Lists
- Q11) C
Relates to: Guidelines for Placing Access Lists
- Q12) A
Relates to: Guidelines for Placing Access Lists
- Q13) C
Relates to: Verifying the Access List Configuration
- Q14) C
Relates to: Verifying the Access List Configuration

Scaling the Network with NAT and PAT

Overview

Two scalability challenges facing the Internet are the depletion of registered IP address space and scaling in routing. Cisco Systems IOS Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. Cisco IOS NAT translates IP addresses within private internal networks to legal IP addresses for transport over public external networks, such as the Internet. Incoming traffic is translated back for delivery within the inside network. This lesson describes the features offered by NAT and shows you how to configure it on Cisco routers.

Relevance

NAT provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of NAT on Cisco routers
- Use Cisco IOS commands to configure NAT, given a functioning router
- Use **show** commands to identify anomalies in the NAT configuration, given an operational router
- Use **debug** commands to identify events and anomalies in the NAT configuration, given an operational router

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

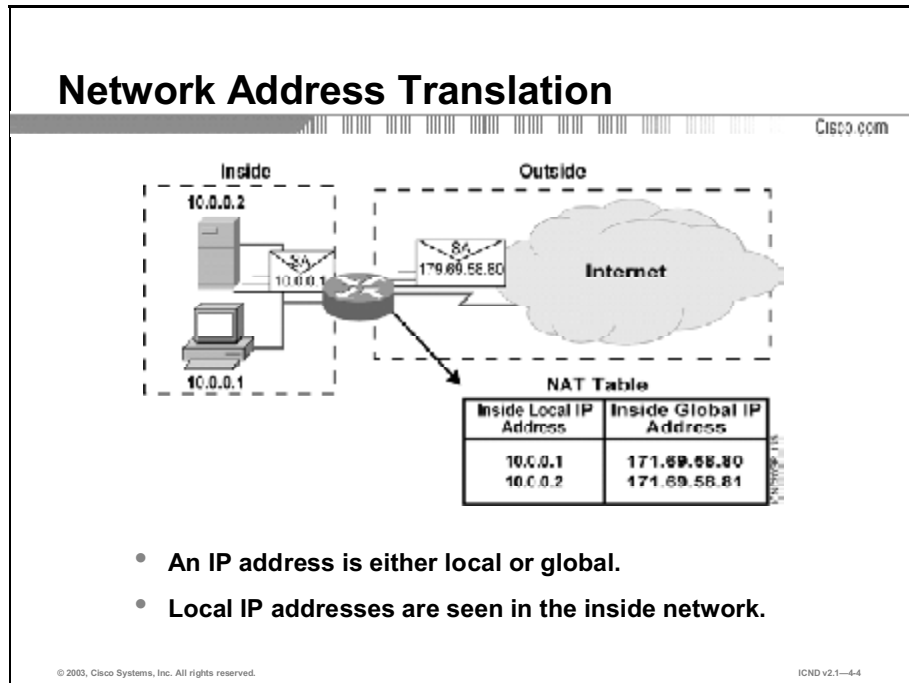
Outline

The lesson includes these topics:

- Overview
- Introducing NAT and PAT
- Translating Inside Source Addresses
- Overloading an Inside Global Address
- Verifying the NAT and PAT Configuration
- Troubleshooting the NAT and PAT Configuration
- Summary
- Quiz

Introducing NAT and PAT

Cisco Systems IOS Network Address Translation (NAT) allows an organization with unregistered private addresses to connect to the Internet by translating those addresses into globally registered IP addresses. Cisco IOS NAT also increases network privacy by hiding internal IP addresses from external networks. Static NAT is designed to allow one-to-one mapping between local and global addresses. Dynamic NAT is designed to map an unregistered IP address to a registered IP address from a group of registered IP addresses. Overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports, known also as port address translation (PAT). This topic describes the capabilities of NAT and PAT.



Cisco NAT is designed for IP address simplification and conservation, as it enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a Cisco router, usually connecting two networks together, and translates the private (inside local) addresses in the internal network to public addresses (inside global) before packets are forwarded to another network. As part of this functionality, you can configure NAT to advertise only one address for the entire network to the outside world. This effectively hides the internal network from the world, thus providing additional security.

A device, such as a firewall, router, or computer, that sits between an internal network and the public network, uses NAT, which is defined in RFC 1631.

In NAT terminology, the *inside network* is the set of networks that are subject to translation. The *outside network* refers to all other addresses. Usually these are valid addresses located on the Internet.

Cisco defines the following NAT terms:

- **Inside local address:** The IP address assigned to a host on the inside network. The address is likely not an IP address assigned by the Network Information Center (NIC) or service provider.
- **Inside global address:** A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
- **Outside local address:** The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.
- **Outside global address:** The IP address assigned to a host on the outside network by the host owner. The address is allocated from a globally routable address or network space.

NAT has many forms and can work in the following ways:

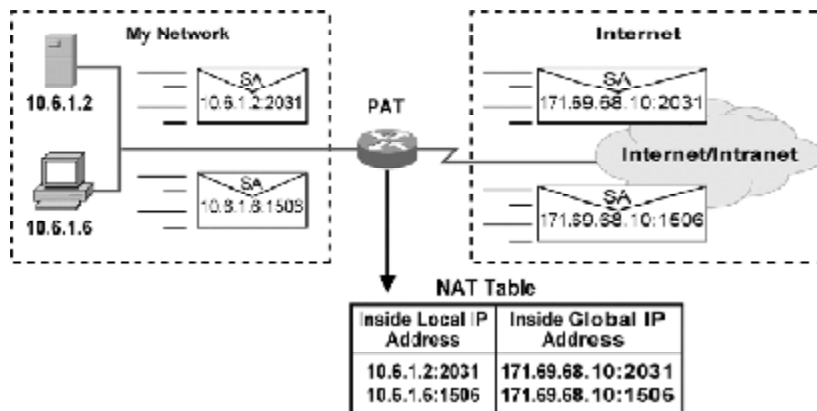
- **Static NAT:** Maps an unregistered IP address to a registered IP address on a one-to-one basis. Static NAT is particularly useful when a device needs to be accessible from outside the network.
- **Dynamic NAT:** Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
- **Overloading:** is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports, known also as PAT (port address translation).

NAT offers the following benefits:

- Eliminates readdressing overhead. NAT eliminates the need to readdress all hosts that require external access, saving time and money.
- Conserves addresses through application port-level multiplexing. With NAT, internal hosts can share a single registered IP address for all external communications. In this type of configuration, relatively few external addresses are required to support many internal hosts, thus conserving IP addresses.
- Protects network security. Because private networks do not advertise their addresses or internal topology, they remain reasonably secure when used in conjunction with NAT to gain controlled external access.

Port Address Translation

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

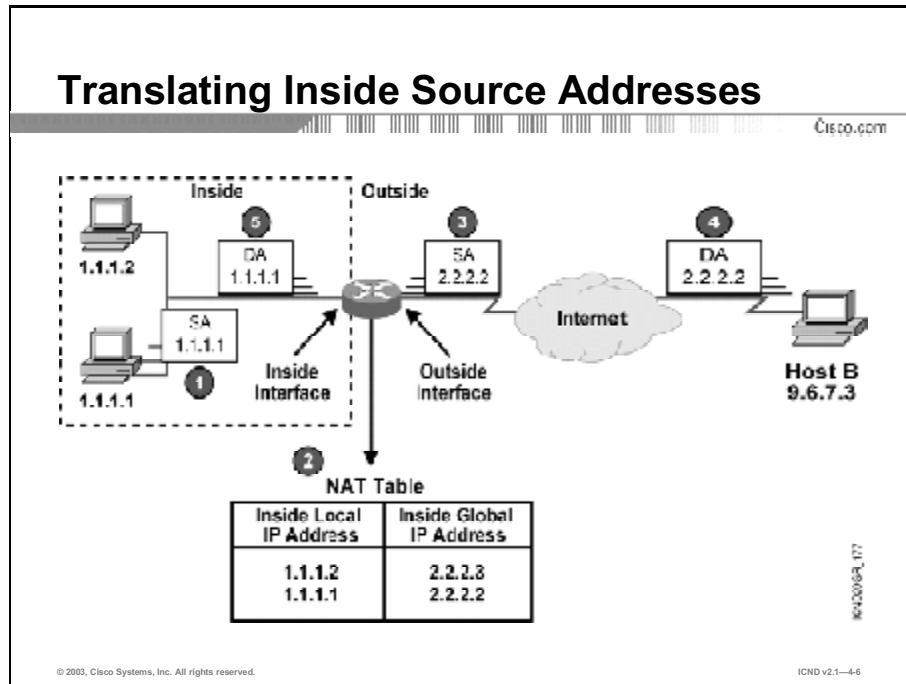
ICND v2.1-4-5

One of the main features of NAT is static PAT, also referred to as “overload” in Cisco IOS configuration. Several internal addresses can be translated using NAT to only one or a few external addresses by using PAT.

PAT uses unique source port numbers on the inside global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number of internal addresses that can be translated using NAT to one external address could theoretically be as many as 65,536 per IP address. PAT will attempt to preserve the original source port. If this source port is already allocated, PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. If there is still no port available from the appropriate port group and more than one external IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and external IP addresses.

Translating Inside Source Addresses

You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network. You can configure static or dynamic inside source translation. This topic shows you how to translate inside source addresses using static and dynamic translation.



The figure illustrates a router that is translating a source address inside a network to a source address outside the network.

The following process describes inside source address translation as shown in the figure:

1. The user at host 1.1.1.1 opens a connection to host B.
2. The first packet that the router receives from host 1.1.1.1 causes the router to check its NAT table.
 - If a static translation entry was configured, the router goes to step 3.
 - If no static translation entry exists, the router determines that source address (SA) 1.1.1.1 must be translated dynamically, selects a legal, global address from the dynamic address pool, and creates a translation entry. This type of entry is called a simple entry.
3. The router replaces the inside local source address of host 1.1.1.1 with the translation entry global address, and forwards the packet.
4. Host B receives the packet and responds to host 1.1.1.1 by using the inside global IP destination address (DA) 2.2.2.2.
5. When the router receives the packet with the inside global IP address, it performs a NAT table lookup by using the inside global address as a key. It then translates the address to the inside local address of host 1.1.1.1 and forwards the packet to host 1.1.1.1.
6. Host 1.1.1.1 receives the packet and continues the conversation. The router performs steps 2 through 5 for each packet.

Configuring Static Translation

Cisco.com

```
Router(config)#ip nat inside source static local-ip global-ip
```

- Establishes static translation between an inside local address and an inside global address.

```
Router(config-if)#ip nat inside
```

- Marks the interface as connected to the inside.

```
Router(config-if)#ip nat outside
```

- Marks the interface as connected to the outside.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-7

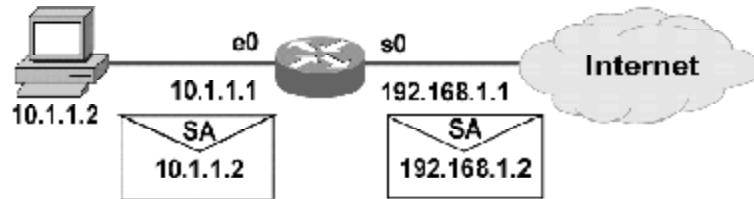
To configure static inside source address translation, perform the following tasks:

Step	Action	Notes
1.	Establish static translation between an inside local address and an inside global address. Router(config)# ip nat inside source static local-ip global-ip	Enter the global no ip nat inside source static command to remove the static source translation.
2.	Specify the inside interface. Router(config)# interface type number	After you enter the interface command, the CLI ¹ prompt will change from (config)# to (config-if)#.
3.	Mark the interface as connected to the inside. Router(config-if)# ip nat inside	
4.	Specify the outside interface. Router(config-if)# interface type number	
5.	Mark the interface as connected to the outside. Router(config-if)# ip nat outside	

¹CLI = command-line interface

Enabling Static NAT Address Mapping Example

Cisco.com



```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-8

The example shows the use of discrete address mapping with static NAT translations. The router will translate packets from host 10.1.1.2 to a source address of 192.168.1.2.

Configuring Dynamic Translation

Cisco.com

```
Router(config)#ip nat pool name start-ip end-ip  
{netmask netmask | prefix-length prefix-length}
```

- Defines a pool of global addresses to be allocated as needed.

```
Router(config)#access-list access-list-number permit  
source [source-wildcard]
```

- Defines a standard IP access list permitting those inside local addresses that are to be translated.

```
Router(config)#ip nat inside source list  
access-list-number pool name
```

- Establishes dynamic source translation, specifying the access list defined in the prior step.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-9

To configure dynamic inside source address translation, perform the following tasks:

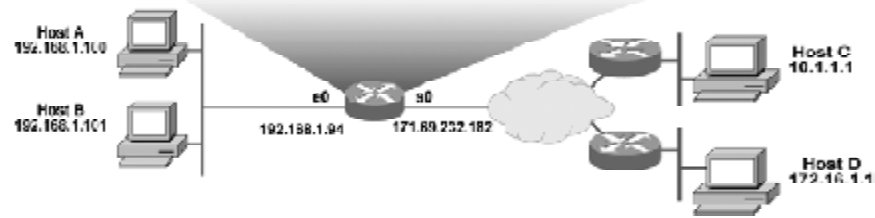
Step	Action	Notes
1.	Define a pool of global addresses to be allocated as needed. Router(config)# ip nat pool name start-ip end-ip { netmask netmask prefix-length prefix-length}	Enter the global no ip nat pool command to remove the pool of global addresses.
2.	Define a standard access list permitting those addresses that are to be translated. Router(config)# access-list access-list-number permit source [source-wildcard]	Enter the global no access-list access-list-number command to remove the access list.
3.	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)# ip nat inside source list access-list-number pool name	Enter the global no ip nat inside source command to remove the dynamic source translation.
4.	Specify the inside interface. Router(config)# interface type number	After you enter the interface command, the CLI prompt will change from (config)# to (config-if)#.
5.	Mark the interface as connected to the inside. Router(config-if)# ip nat inside	
6.	Specify the outside interface. Router(config-if)# interface type number	
7.	Mark the interface as connected to the outside. Router(config-if)# ip nat outside	

Caution The access list must permit only those addresses that are to be translated. Remember that there is an implicit *deny all* at the end of each access list. An access list that is too permissive can lead to unpredictable results. Cisco highly recommends that you do not configure access lists referenced by NAT commands with *permit any*. Using permit any can result in NAT consuming too many router resources, which can cause network problems.

Dynamic Address Translation Example

Cisco.com

```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
```



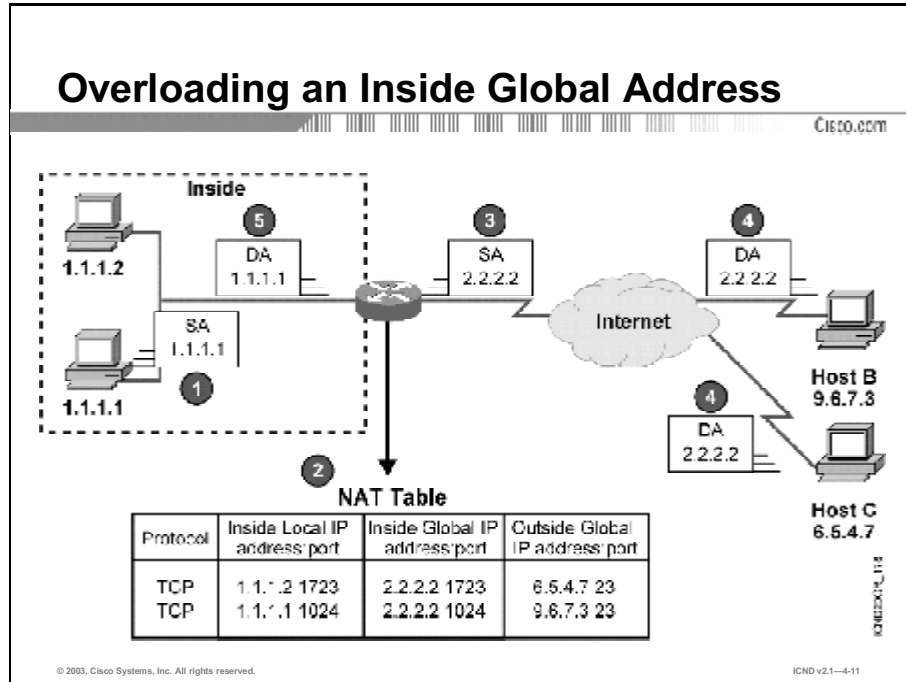
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-10

The example translates all source addresses passing access list 1 (having a source address from 192.168.1.0/24) to an address from the pool named net-208. The pool contains addresses from 171.69.233.209/28 to 171.69.233.222/28.

Overloading an Inside Global Address

One of the main features of NAT is static PAT, also referred to as “overload” in Cisco IOS configuration. This topic explains how to configure PAT by overloading an inside global address.



You can conserve addresses in the inside global address pool by allowing the router to use one inside global address for many inside local addresses. When this overloading is configured, the router maintains enough information from higher-level protocols (for example, TCP or User Datagram Protocol [UDP] port numbers) to translate the inside global address back to the correct inside local address. When multiple inside local addresses map to one inside global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

The figure illustrates NAT operation when one inside global address represents multiple inside local addresses. The TCP port numbers act as differentiators. Both host B and host C think they are talking to a single host at address 2.2.2.2. They are actually talking to different hosts; the port number is the differentiator. In fact, many inside hosts could share the inside global IP address by using many port numbers.

The router performs the following process in overloading inside global addresses:

1. The user at host 1.1.1.1 opens a connection to host B.
2. The first packet that the router receives from host 1.1.1.1 causes the router to check its NAT table.

If no translation entry exists, the router determines that address 1.1.1.1 must be translated, and sets up a translation of inside local address 1.1.1.1 to a legal inside global address. If overloading is enabled, and another translation is active, the router reuses the inside global

address from that translation and saves enough information to be able to translate back. This type of entry is called an extended entry.

3. The router replaces the inside local source address 1.1.1.1 with the selected inside global address and forwards the packet.
4. Host B receives the packet and responds to host 1.1.1.1 by using the inside global IP address 2.2.2.2.
5. When the router receives the packet with the inside global IP address, it performs a NAT table lookup. Using the inside global address and port, and outside global address and port as a key, it translates the address into inside local address 1.1.1.1, and forwards the packet to host 1.1.1.1.
6. Host 1.1.1.1 receives the packet and continues the conversation. The router performs steps 2 through 5 for each packet.

Configuring Overloading

Cisco.com

```
Router(config)#access-list access-list-number permit  
source source-wildcard
```

- Defines a standard IP access list permitting those inside local addresses that are to be translated

```
Router(config)#ip nat inside source list  
access-list-number interface interface overload
```

- Establishes dynamic source translation, specifying the access list defined in the prior step

© 2003, Cisco Systems, Inc. All rights reserved.

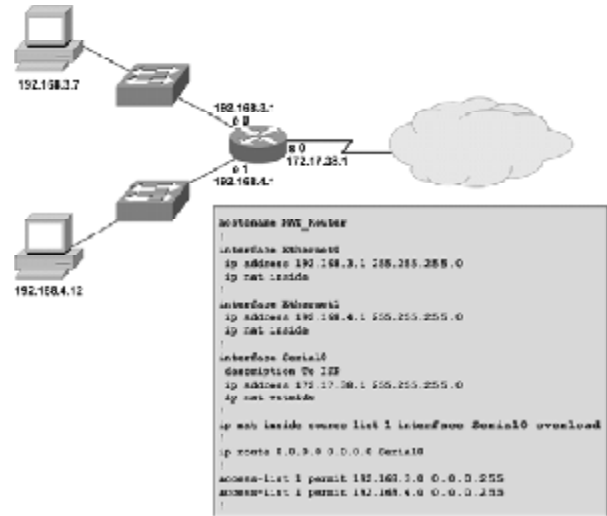
ICND v2.1—4-12

To configure overloading of inside global addresses, perform the following tasks:

Step	Action	Notes
1.	Define a standard access list permitting those addresses that are to be translated. Router(config)# access-list access-list-number permit source [source-wildcard]	Enter the global no access-list access-list-number command to remove the access list.
2.	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)# ip nat inside source list access-list-number interface interface overload	Enter the global no ip nat inside source command to remove the dynamic source translation. The overload keyword enables PAT.
3.	Specify the inside interface. Router(config)# interface type number Router(config-if)# ip nat inside	After you enter the interface command, the CLI prompt will change from (config)# to (config-if)#.
4.	Specify the outside interface. Router(config-if)# interface type number Router(config-if)# ip nat outside	

Overloading an Inside Global Address Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-13

The NAT inside-to-outside process works in this sequence:

1. The incoming packet goes to route table and the next hop is identified.
2. NAT statements are parsed to use the interface Serial 0 IP address in overload mode, using PAT to create a source address to use.
3. The router encapsulates the packet and sends it out on interface Serial 0.
4. The NAT outside-to-inside address translation process works in sequence.
5. NAT statements are parsed. The router looks for an existing translation and identifies the appropriate destination address.
6. The packet goes to the route table and the next hop interface is determined.
7. The packet is encapsulated and sent out to the local interface.

This example is simple to configure and understand. No internal addresses are visible; therefore hosts do not have an external public address, which leads to improved security.

Verifying the NAT and PAT Configuration

After you have configured NAT, verify that it is operating as expected. You can do this by using the **clear** and **show** commands. This topic explains how to verify the NAT and PAT configuration.

Clearing the NAT Translation Table

CISCO.COM

```
Router#clear ip nat translation *
```

- Clears all dynamic address translation entries

```
Router#clear ip nat translation inside global-ip  
local-ip [outside local-ip global-ip]
```

- Clears a simple dynamic translation entry containing an inside translation, or both inside and outside translation

```
Router#clear ip nat translation outside  
local-ip global-ip
```

- Clears a simple dynamic translation entry containing an outside translation

```
Router#clear ip nat translation protocol inside global-ip  
global-port local-ip local-port [outside local-ip  
local-port global-ip global-port]
```

- Clears an extended dynamic translation entry

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-14

By default, dynamic address translations will time out from the NAT translation table at some point. Dynamic translations time out after a period of nonuse. When port translation is not configured, translation entries time out after 24 hours, unless you reconfigure them with the **ip nat translation** command. You can clear the entries before the timeout by using one of the following commands:

Command	Description
<code>clear ip nat translation *</code>	Clears all dynamic address translation entries from the NAT translation table.
<code>clear ip nat translation inside global-ip local-ip [outside local-ip global-ip]</code>	Clears a simple dynamic translation entry containing an inside translation, or both inside and outside translation.
<code>clear ip nat translation outside local-ip global-ip</code>	Clears a simple dynamic translation entry containing an outside translation.
<code>clear ip nat translation protocol inside global-ip global-port local-ip local-port [outside local-ip local-port global-ip global-port]</code>	Clears an extended dynamic translation entry.

Displaying Information with show Commands

Cisco.com

```
Router#show ip nat translations
```

- Displays active translations

```
Router#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.131.1        10.10.10.1         ---                ---
```

```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic, 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 5 Misses: 0
...
```

© 2003, Cisco Systems, Inc. All rights reserved.

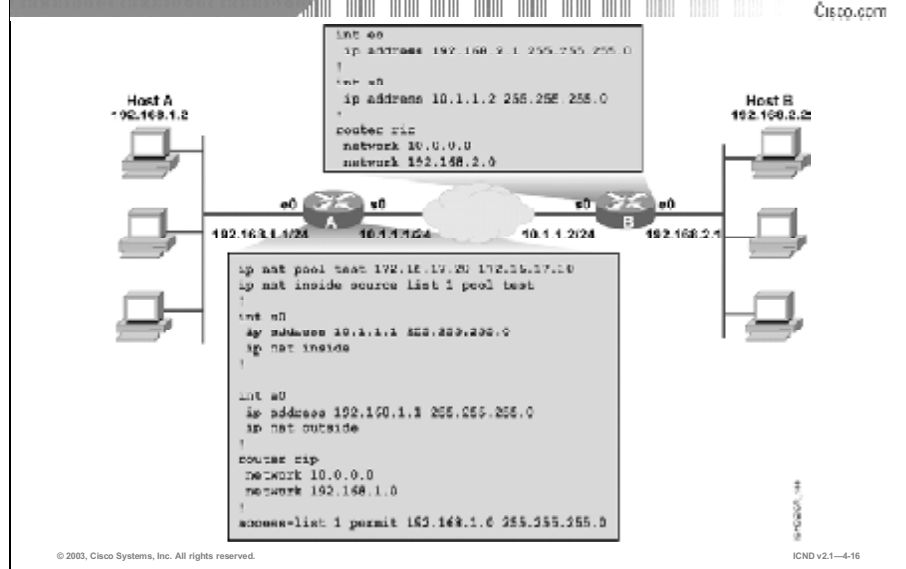
ICND v2.1—4-15

You can display translation information by performing one of the following tasks in EXEC mode:

Command	Description
<code>show ip nat translations</code>	Displays active translations.
<code>show ip nat statistics</code>	Displays translation statistics.

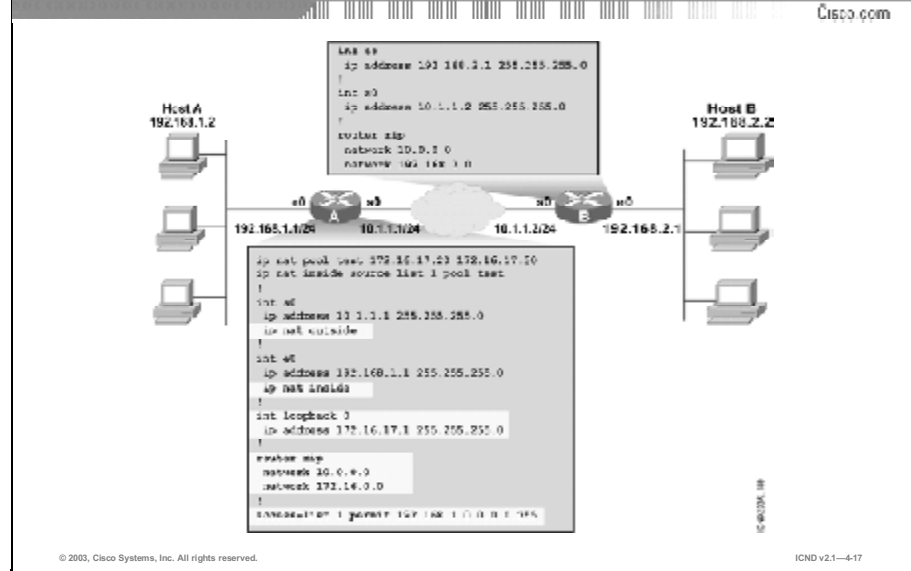
Alternatively, you can use the **show run** command and look for NAT, access list, interface, or pool commands with the required values.

Sample Problem: Cannot Ping Remote Host



In the figure, the network administrator is experiencing the following symptom: host A (192.168.1.2) cannot ping host B (192.168.2.2).

Solution: New Configuration



To fix the error, you need to change the router A configuration as follows:

- Configure interface S0 to be the outside interface, rather than the inside interface.
- Configure interface E0 to be the inside interface, rather than the outside interface.
- Configure router A to advertise network 172.16.0.0. Previously, router B did not know how to reach the 172.16.17.0/24 subnet.
- Configure the wildcard mask to match any host on the 192.168.1.0 network. Previously, the **access-list 1** command did not match any inside local IP address.

Troubleshooting the NAT and PAT Configuration

When you have IP connectivity problems in a NAT environment, it is often difficult to determine the cause of the problem. Many times NAT is mistakenly blamed, when in reality there is an underlying problem. This topic explains how to verify NAT operation using tools that are available on Cisco routers.

Using the debug ip nat Command

Cisco.com

```
Router#debug ip nat
```

```
NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1-4-18

When trying to determine the cause of an IP connectivity problem, it helps to rule out NAT. Follow these steps to verify that NAT is operating as expected:

- Step 1** Based on the configuration, clearly define what NAT is supposed to achieve. You may determine that there is a problem with the configuration.
- Step 2** Verify that correct translations exist in the translation table.
- Step 3** Verify the translation is occurring by using **show** and **debug** commands.
- Step 4** Review in detail what is happening to the packet and verify that routers have the correct routing information to move the packet along.

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also outputs information about certain errors or exception conditions, such as the failure to allocate a global address.

The figure shows sample **debug ip nat** output. In this example, the first two lines show the debugging output that a Domain Name System (DNS) request and reply produced. The remaining lines show the debugging output from a Telnet connection, from a host on the inside of the network to a host on the outside of the network.

The asterisk next to NAT indicates that the translation is occurring in the fast-switched path. The first packet in a conversation will always be process switched. The remaining packets will go through the fast-switched path if a cache entry exists.

The final entry in each line, in brackets ([]), provides the identification number of the packet. This information might be useful in the debugging process to correlate with other packet traces from protocol analyzers.

Translation Not Installed in the Translation Table?

Cisco.com

- **Verify that:**
 - **The configuration is correct.**
 - **There are not any inbound access lists denying the packets from entering the NAT router.**
 - **The access list referenced by the NAT command is permitting all necessary networks.**
 - **There are enough addresses in the NAT pool.**
 - **The router interfaces are appropriately defined as NAT inside or NAT outside.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—4-19

To determine if the appropriate translation is installed in the translation table, verify the items shown in the figure.

Summary

This topic summarizes the key points discussed in this lesson.

Summary



- **Cisco IOS NAT allows an organization with unregistered private addresses to connect to the Internet by translating those addresses into globally registered IP addresses.**
- **You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network.**
- **Overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different ports, known also as PAT.**
- **Once you have configured NAT, verify that it is operating as expected using the clear and show commands.**
- **Sometimes NAT is blamed for IP connectivity problems when there is actually a routing problem.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—4-20

References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

Next Steps

After completing this lesson, go to:

- Lab Exercise 4-1: Configuring IP Access Lists
- Lab Exercise 4-2: Configuring Port Address Translation

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which two benefits describe NAT? (Choose two.)
- A) protects network security
 - B) increases readdressing resources
 - C) reduces the number of ports required for Internet connectivity
 - D) conserves addresses through application port-level multiplexing
- Q2) PAT uses unique _____ on the inside global IP address to distinguish between translations.
- A) address pools
 - B) protocol numbers
 - C) source port numbers
 - D) destination IP addresses
- Q3) Which Cisco IOS command would you use to establish static translation between an inside local address and an inside global address?
- A) **ip nat pool**
 - B) **ip nat inside**
 - C) **ip nat outside**
 - D) **ip nat inside source static**
- Q4) What does the **ip nat outside** command configure?
- A) marks the interface as connected to the outside
 - B) creates a pool of global addresses to be allocated as needed
 - C) establishes static translation between a local address and a global address
 - D) establishes dynamic translation between an outside local address and an outside global address

- Q5) What is the complete command to create a pool of NAT addresses with the following parameters?
- pool name is pool1
 - range of pool addresses is 192.166.25.17 to 192.166.25.30
 - net mask is 255.255.255.240
- A) **ip nat pool pool1 192.166.25.17 192.166.25.30**
- B) **ip nat pool 192.166.25.17 192.166.125.30 255.255.255.240 pool1**
- C) **ip nat pool pool1 192.166.25.17 192.166.25.30 netmask 255.255.255.240**
- D) **ip nat pool pool1 netmask 255.255.255.240 192.166.25.17 192.166.25.30**
- Q6) When you use the **ip nat inside source** command, what does the overload option do?
- A) enables PAT
- B) enables NAT
- C) defines an outside global address
- D) defines a pool of global addresses
- Q7) Which command clears all dynamic address translation entries from the NAT translation table?
- A) **clear ip nat translation ***
- B) **clear ip nat translation inside**
- C) **clear ip nat translation outside**
- D) **clear ip nat translation protocol inside**
- Q8) Which command clears a simple dynamic translation entry containing an outside translation?
- A) **clear ip nat translation ***
- B) **clear ip nat translation inside**
- C) **clear ip nat translation outside**
- D) **clear ip nat translation protocol inside**
- Q9) Before using **show** and **debug** commands to determine the cause of an IP connectivity problem, what should you do?
- A) Clearly define what NAT is supposed to achieve.
- B) Use the **debug ip nat** command to determine if there is a problem to investigate.
- C) Verify that the correct translations exist in the translation table, using **show** commands.
- D) Review what is happening to each packet and verify that routers have the correct routing information.

- Q10) Use the _____ command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router.
- A) **debug ip nat**
 - B) **debug ip nat ~~verbose~~**
 - C) **show ip nat statistics**
 - D) **show ip nat translations**

Quiz Answer Key

- Q1) A, D
Relates to: Introducing NAT and Port Address Translation
- Q2) C
Relates to: Introducing NAT and Port Address Translation
- Q3) D
Relates to: Translating Inside Source Addresses
- Q4) A
Relates to: Translating Inside Source Addresses
- Q5) C
Relates to: Overloading an Inside Global Address
- Q6) A
Relates to: Overloading an Inside Global Address
- Q7) A
Relates to: Verifying the NAT and Port Address Translation Configuration
- Q8) C
Relates to: Verifying the NAT and Port Address Translation Configuration
- Q9) C
Relates to: Troubleshooting the NAT and Port Address Translation Configuration
- Q10) A
Relates to: Troubleshooting the NAT and Port Address Translation Configuration

Lesson Assessments

Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

Outline

This section includes these assessments:

- Lesson Assessment 4-1: Access Lists and Their Applications
- Lesson Assessment 4-2: Configuring IP Access Lists
- Lesson Assessment 4-3: Scaling the Network with NAT and PAT

Lesson Assessment 4-1: Access Lists and Their Applications

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Explain the purpose of access lists and identify potential applications
- Describe how Cisco IOS software processes standard and extended access lists on inbound and outbound interfaces

Quiz

Answer these questions:

- Q1) Which three statements best describe the uses for access lists on Cisco routers? (Choose three.)
- A) You can use access lists to identify traffic for dial-on-demand routing.
 - B) You can use access lists to classify traffic for priority or custom queuing.
 - C) You can use access lists to permit or deny packets moving through the router.
 - D) You can use access lists to authenticate passwords to gain access to the router.
 - E) You can use access lists to permit or deny traffic that originated from the router itself.
- Q2) When does an inbound access list check packets on a Cisco router?
- A) as they arrive at the router
 - B) after the router authenticates the packets
 - C) after they are processed by the routing table
 - D) before they are sent onto a network from the router
- Q3) An IP access list is a sequential list of _____ that apply to IP addresses or upper-layer IP protocols.
- A) passwords
 - B) usernames and passwords
 - C) permit and deny conditions
 - D) Cisco IOS permit statements
- Q4) What does a Cisco router do with a packet when it matches an access list *permit* statement?
- A) It discards the packet.
 - B) It returns the packet to its originator.
 - C) It sends the packet to the output buffer.
 - D) It holds the packet for further processing.

- Q5) What does a Cisco router do with a packet when it matches an access list entry statement?
- A) It discards the packet.
 - B) It returns the packet to its originator.
 - C) It sends the packet to the output buffer.
 - D) It holds the packet for further processing.
- Q6) When discarding packets, some protocols return _____ to notify the sender that the destination is unreachable.
- A) nothing
 - B) the packet
 - C) a special packet
 - D) a delivery notification
- Q7) You can apply an access list to multiple interfaces. How many access lists per protocol, per direction, per interface can you apply?
- A) 1
 - B) 2
 - C) 4
 - D) any number
- Q8) What is the term for the final default statement at the end of every access list?
- A) implicit deny all
 - B) implicit deny host
 - C) implicit permit any
 - D) implicit permit host
- Q9) Which statement best describes the difference between standard and extended access lists?
- A) Standard access lists use the range 100 through 149 while extended access lists use the range 150 through 199.
 - B) Standard access lists use filters based on the source and destination while extended access lists filter based on source address.
 - C) Standard access lists permit or deny access to a specified well-known port while extended access lists filter based on source address and mask.
 - D) Standard access lists permit or deny the entire TCP/IP protocol suite while extended access lists can specify a specific IP protocol and port number.
- Q10) Which two ranges of numbers can you use to identify IP extended access lists on a Cisco router? (Choose two.)
- A) 1 to 99
 - B) 51 to 151
 - C) 100 to 199
 - D) 200 to 299
 - E) 1300 to 1999
 - F) 2000 to 2699

- Q11) If you set the wildcard mask to 00111111, what does the Cisco router do?
- A) ignores the last 6 address bits
 - B) checks all address bits (match all)
 - C) ignores the most significant 2 address bits
 - D) does not check the address (ignores bits in octet)

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Lesson Assessment 4-2: Configuring IP Access Lists

Complete this quiz to assess what you learned in the lesson.

Objectives

This quiz tests your knowledge of how to:

- Use Cisco IOS commands to configure standard and extended access lists, given a functioning router
- Use **show** commands to identify anomalies in IP standard and extended access lists, given an operational router

Quiz

Answer these questions:

- Q1) Which statement about access lists is true?
- A) Access lists are processed from bottom up.
 - B) All access lists end with an implicit deny all statement.
 - C) The order of access list statements is not important to proper filtering.
 - D) Standard access lists allow removal and reordering of individual statements from a list.
- Q2) What does the last global statement in an access list specify?
- A) deny term
 - B) permit term
 - C) access list number
 - D) access list test conditions
- Q3) A system administrator wants to configure an IP standard access list on a Cisco router to allow only packets from all hosts on the subnet 10.1.1.0/24 from entering the ethernet0 interface of the router. Which configuration accomplishes this goal?
- A) **access-list 1 permit 10.1.1.0**
 - B) **access-list 1 permit 10.1.1.0 host**
 - C) **access-list 99 permit 10.1.1.0 0.0.0.255**
 - D) **access-list 100 permit 10.1.1.0 0.0.0.255**
- Q4) Which Cisco IOS command links an extended IP access list to an interface?
- A) **ip access-list 101 e0**
 - B) **access-group 101 e0**
 - C) **ip access-group 101 in**
 - D) **access-list 101 permit tcp access-list 100 permit 10.1.1.0 0.0.0.255 eq 21**

- Q5) What is the complete command to create an access list entry with the following parameters:
- Source IP address is 172.16.0.0
 - Source mask is 0.0.255.255
 - Permit this entry
 - Access list number is 1
- A) **access-list 1 deny 172.16.0.0 0.0.255.255**
B) **access-list 1 permit 172.16.0.0 0.0.255.255**
C) **access-list permit 1 172.16.0.0 255.255.0.0**
D) **access-list 99 permit 172.16.0.0 0.0.255.255**
- Q6) The following is an access-list entered on a Cisco router.
- ```
access-list 135 deny tcp 172.16.16.0 0.0.15.255 172.16.32.0 0.0.15.255
eq telnet
access-list 135 permit ip any any
```
- If this access list is used to control incoming packets on ethernet0, which three statements are true? (Choose three.)
- A) Address 172.16.1.1 will be denied telnet access to address 172.16.37.5.  
B) Address 172.16.31.1 will be permitted FTP access to address 172.16.45.1.  
C) Address 172.16.1.1 will be permitted Telnet access to address 172.16.32.1.  
D) Address 172.16.16.1 will be permitted Telnet access to address 172.16.32.1.  
E) Address 172.16.16.1 will be permitted Telnet access to address 172.16.50.1.  
F) Address 172.16.30.12 will be permitted Telnet access to address 172.16.32.12.
- Q7) A system administrator has created a ten-line standard access list with the identifier 120 on a Cisco router. There is an error in the fifth line and this line needs to be replaced. How can the system administrator fix this problem?
- A) The system administrator can delete the fifth line and then reenter it.  
B) The system administrator will have to delete all lines in the access list. All lines will then need to be reentered.  
C) The system administrator can delete each line, starting at the end of the list, until the incorrect line is deleted. The last five lines then need to be reentered.  
D) The system administrator can delete each line, starting at the beginning of the list, until the incorrect line is deleted. The first five lines then need to be reentered.
- Q8) Which command applies standard IP access list filtering to vty lines for an outgoing Telnet session originating from within a router?
- A) **access-vty 1 out**  
B) **access-class 1 out**  
C) **ip access-list 1 out**  
D) **ip access-group 1 out**

- Q9) Access lists are processed from the top down. If you place the more specific tests, and tests that will test true frequently, in the beginning of the access list, you can \_\_\_\_.
- A) reduce processing overhead
  - B) use the access list for other routers
  - C) make it more easily edit access lists
  - D) insert the less specific tests more easily
- Q10) To provide optimal packet filtering, what should you do?
- A) Reorder the access list statements frequently.
  - B) Place more specific tests at the beginning of the access list.
  - C) Include an implicit deny statement at the end of each access list.
  - D) Use named access lists so that you can reorder individual statements as needed.
- Q11) Which command is used on a Cisco router to determine if IP access lists are applied to an Ethernet interface?
- A) **show interfaces**
  - B) **show access list**
  - C) **show ip interface**
  - D) **show ip access-list**
- Q12) Which command is used to find out if access list 300 has been configured on a Cisco router?
- A) **show interfaces**
  - B) **show ip interface**
  - C) **show ip access-list**
  - D) **show access-groups**

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment 4-3: Scaling the Network with NAT and PAT

Complete this quiz to assess what you learned in the lesson.

## Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of NAT on Cisco routers
- Use Cisco IOS commands to configure NAT, given a functioning router
- Use **show** commands to identify anomalies in the NAT configuration, given an operational router
- Use **debug** commands to identify events and anomalies in the NAT configuration, given an operational router

## Quiz

Answer these questions:

Q1) Match each NAT term to its definition.

- |       |    |                           |
|-------|----|---------------------------|
| _____ | 1. | static NAT                |
| _____ | 2. | dynamic NAT               |
| _____ | 3. | inside network            |
| _____ | 4. | outside global IP address |
- A) set of networks subject to translation using NAT
- B) IP address of an inside host as it appears to the outside network (the “translated IP address”)
- C) form of NAT that maps an unregistered IP address to a registered IP address on a one-to-one basis
- D) form of NAT that maps an unregistered IP address to a registered IP address from a group of registered IP addresses

Q2) One of the main features of NAT is \_\_\_\_\_, also referred to as “overload” in Cisco IOS configuration.

- A) port address translation
- B) static address translation
- C) protocol address translation
- D) dynamic address translation

- Q3) Which Cisco IOS command would you use to define a pool of global addresses to be allocated as needed?
- A) **ip nat pool**
  - B) **ip nat inside pool**
  - C) **ip nat outside pool**
  - D) **ip nat inside source static**
- Q4) What does the **ip nat inside source static** command configure?
- A) selects the outside interface
  - B) marks the interface as connected to the outside
  - C) creates a pool of global addresses to be allocated as needed
  - D) establishes static translation between an inside local address and an inside global address
- Q5) Match each command used to configure NAT overloading to its function.
- |          |                                                                           |
|----------|---------------------------------------------------------------------------|
| _____ 1. | <b>ip nat inside</b>                                                      |
| _____ 2. | <b>ip nat outside</b>                                                     |
| _____ 3. | <b>access-list 1 permit 10.1.1.0 0.0.0.255</b>                            |
| _____ 4. | <b>ip nat inside source list 1 pool nat-pool overload</b>                 |
| _____ 5. | <b>ip nat pool nat-pool 192.1.1.17 192.1.1.20 netmask 255.255.255.240</b> |
- A) marks an interface as connected to the inside
  - B) marks an interface as connected to the outside
  - C) defines a pool of inside global addresses to be allocated as needed
  - D) establishes dynamic port address translation using the defined access list
  - E) defines a standard access list permitting the addresses that are to be translated
- Q6) Which command clears an extended dynamic translation entry from the NAT translation table?
- A) **clear ip nat translation \***
  - B) **clear ip nat translation inside**
  - C) **clear ip nat translation outside**
  - D) **clear ip nat translation protocol inside**
- Q7) To make sure that NAT translation is taking place in a router, which Cisco IOS command should you use first?
- A) **debug ip nat**
  - B) **show ip nat statistics**
  - C) **clear ip nat statistics**
  - D) **port address translation**

- Q8) Which command displays the active translations for a NAT translation table?
- A) **show ip nat statistics**
  - B) **show ip nat translations**
  - C) **clear ip nat translation \***
  - D) **clear ip nat translation outside**
- Q9) Suppose you are troubleshooting an IP connectivity problem on a Cisco router and you determine that the appropriate translation is not installed in the translation table. Which three actions should you take? (Choose three.)
- A) Determine if there are enough addresses in the NAT pool.
  - B) Run **debug ip nat *detailed*** to determine the source of the problem.
  - C) Use the **show ip route** command to verify that the selected route exists.
  - D) Verify that the router interfaces are appropriately defined as NAT inside or NAT outside.
  - E) Verify that the access list referenced by the NAT command is permitting all necessary inside local IP addresses.
- Q10) The \_\_\_\_\_ command outputs information about certain errors or exceptional conditions, such as the failure to allocate a global address.
- A) **debug ip nat**
  - B) **debug ip nat *detailed***
  - C) **show ip nat statistics**
  - D) **show ip nat translations**

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment Answer Key

## Lesson Assessment 4-1: Access Lists and Their Applications

- Q1) A, B, C
- Q2) A
- Q3) C
- Q4) C
- Q5) A
- Q6) C
- Q7) A
- Q8) A
- Q9) D
- Q10) C, F
- Q11) A

## Lesson Assessment 4-2: Configuring IP Access Lists

- Q1) B
- Q2) D
- Q3) C
- Q4) C
- Q5) B
- Q6) B, C, E
- Q7) B
- Q8) B
- Q9) A
- Q10) B
- Q11) C
- Q12) C

## Lesson Assessment 4-3: Scaling the Network with NAT and PAT

- Q1) C, D, A, B
- Q2) A
- Q3) A
- Q4) D
- Q5) A, B, E, D, C
- Q6) D
- Q7) C
- Q8) B
- Q9) A, D, E
- Q10) B





# Establishing Serial Point-to-Point Connections

---

## Overview

PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. In addition to IP, PPP supports other network-layer protocols including Internetwork Packet Exchange (IPX) and AppleTalk. This module describes how to configure serial interfaces using PPP and High-Level Data Link Control (HDLC) encapsulation.

Upon completing this module, you will be able to:

- Use Cisco IOS commands to configure serial interfaces using HDLC and PPP encapsulation for leased-line connections, given a functioning router
- Use **show** commands to identify anomalies in HDLC and PPP encapsulation for leased-line connections, given an operational router
- Use **debug** commands to identify events and anomalies in HDLC and PPP encapsulation for leased-line connections, given an operational router

## Outline

The module contains these lessons:

- Wide-Area Networking Review
- Configuring Serial Point-to-Point Encapsulation
- Lesson Assessments



# Wide-Area Networking Review

---

## Overview

Wide-area networking services are typically leased from a service provider. The connection between your network and the service provider network is commonly made with a serial point-to-point connection. This lesson describes the features and components of a WAN and discusses the cabling and protocol requirements for making WAN connections.

## Relevance

Before you configure serial point-to-point to connections, it is helpful to know the purpose of such connections in the context of a WAN.

## Objectives

Upon completing this lesson, you will be able to:

- Describe leased-line, circuit-switched, and packet-switched networks
- Define terms used by WAN service providers, including customer premises equipment, demarcation, local loop, central office, and toll network
- Identify the five serial standards supported by Cisco devices
- Describe the major WAN protocols including High-Level Data Link Control, PPP, Serial Line Internet Protocol, X.25, Frame Relay, and ATM

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

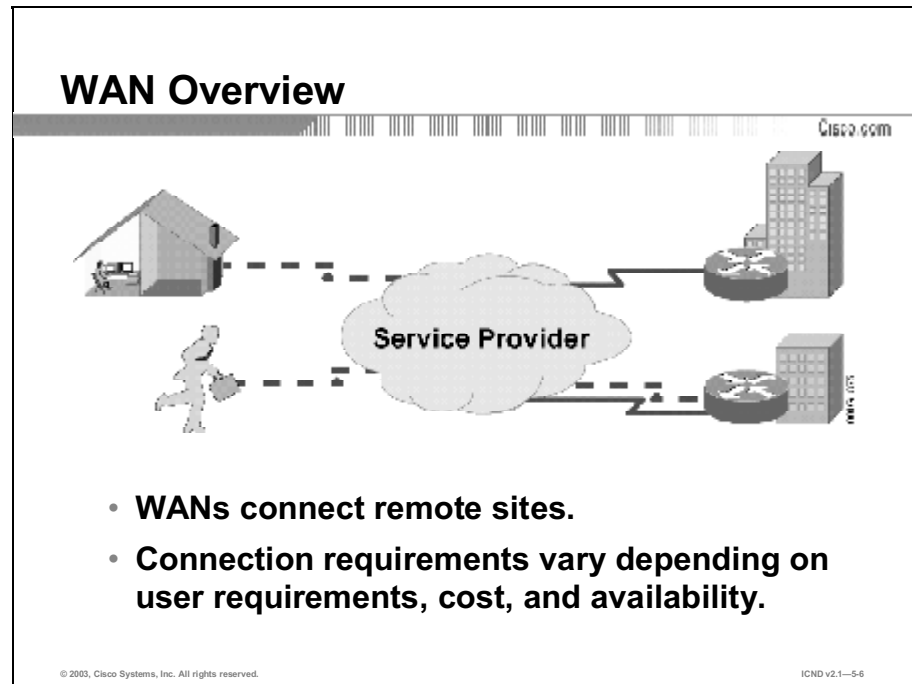
## Outline

The lesson includes these topics:

- Overview
- WAN Review
- WAN Connection Types
- WAN Cabling
- Layer 2 Encapsulation Protocols
- Summary
- Quiz

# WAN Review

A WAN makes data connections across a broad geographic area so that information can be exchanged between distant sites. This topic defines the characteristics of a WAN.



A WAN is different from a LAN. Unlike a LAN, which connects workstations, peripherals, terminals, and other devices in a single building or other small geographic area, a WAN makes data connections across a broad geographic area. Companies use the WAN to connect various company sites so that information can be exchanged between distant offices.

Because the cost of building a global network to connect remote sites can be astronomical, WAN services are generally leased from service providers. You must subscribe to an outside WAN provider to use network resources that your organization does not own. The service provider will use the portion of its network that you leased to transport the information.

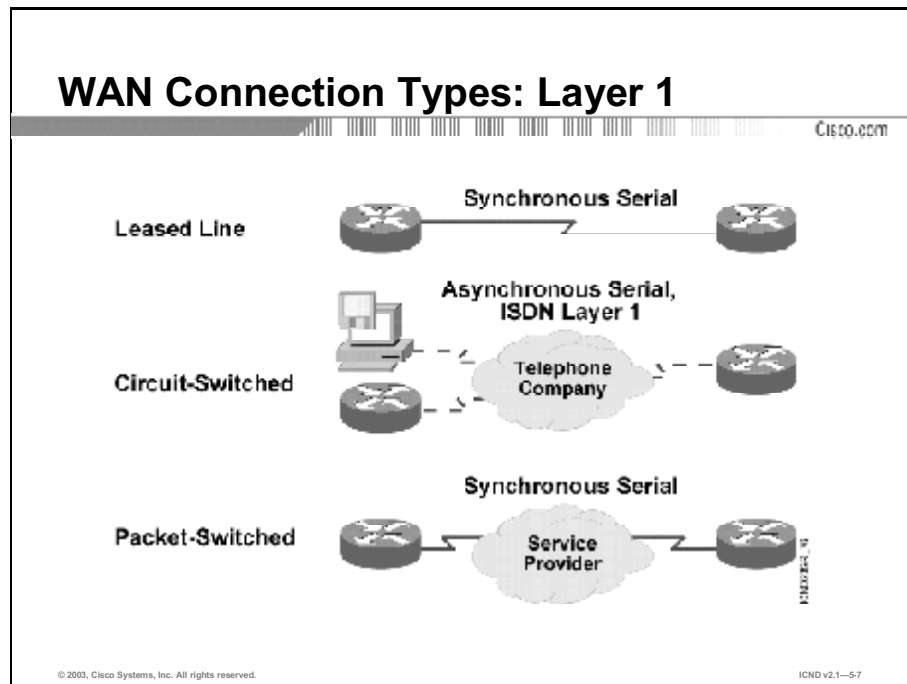
---

**Note** A metropolitan-area network (MAN) leverages the high-speed communication infrastructure built around large cities. A MAN supports higher bandwidth than is typically afforded by a WAN, but is limited in scope to the high-speed infrastructure contained in the metropolitan area.

---

# WAN Connection Types

Some of the WAN connection types available are leased line, circuit-switched, and packet-switched. This topic describes the different WAN connection types and the components that provide the connection.

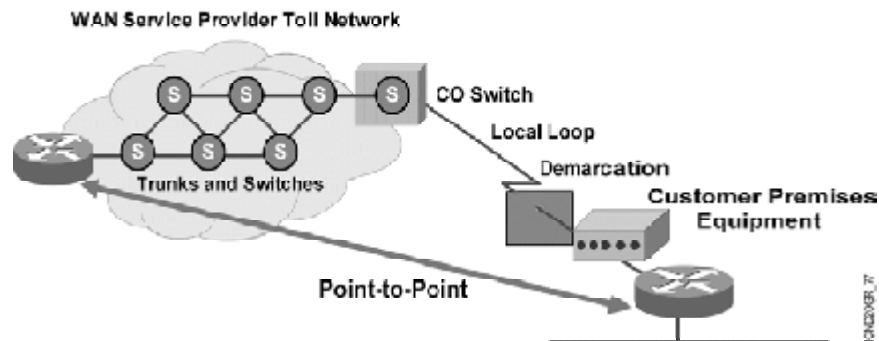


Some of the WAN connection types that you can select are as follows:

- **Leased line:** A leased line, also known as a point-to-point or dedicated connection, provides a single, preestablished WAN communications path from the customer premises, through a service provider network, to a remote network. The service provider reserves this connection for private use by the client. Leased lines eliminate the issues that arise with a shared connection, but they are costly. Leased lines are typically employed over synchronous serial connections up to T3 speeds, operating at 45 Mbps.
- **Circuit-switched:** Circuit switching is a switching system in which a dedicated circuit path must exist between sender and receiver for the duration of the “call.” Service provider networks use circuit switching to provide basic telephone service or ISDN. Circuit-switched connections are commonly used in environments that require only sporadic WAN usage. Basic telephone service is typically employed over an asynchronous serial connection.
- **Packet-switched:** Packet switching is a WAN switching method in which network devices share a common backbone to transport packets from a source to a destination across a carrier network. Packet-switched networks use virtual circuits (VCs) that provide end-to-end connectivity. Programmed switching devices provide the physical connections. Packet headers generally identify the destination. Packet switching offers services similar to those of leased lines; however, the line is shared and the cost of the service is lower. Like leased lines, packet-switched networks are often employed over serial connections with speeds ranging from 56 kbps to T3 speeds (45 Mbps). Cell switching is similar to packet switching, but instead of packets, data is divided into fixed-length cells and then transported across VCs. Cell-switched connections can range in speed from T1 (1.544 Mbps) to DS-3 (45 Mbps) using copper cabling, and up to OC-192 (10 Gbps) using fiber cabling.

## Interfacing Between WAN Service Providers

Cisco.com



- **Provider assigns connection parameters to subscriber.**

© 2003, Cisco Systems, Inc. All rights reserved.

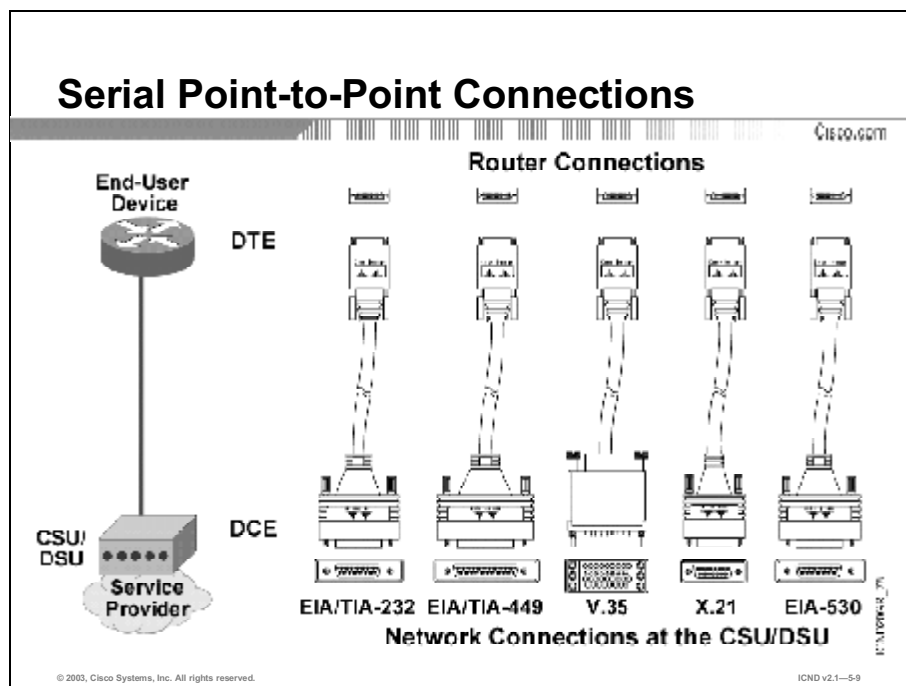
ICND v2.1—5-8

When your organization subscribes to an outside WAN service for network resources, the provider assigns your organization the parameters for making the WAN link. Commonly used terms for the main physical parts are as follows:

- **Customer premises equipment (CPE):** Devices physically located on subscriber premises. The equipment includes devices that are owned by the subscriber and devices that are leased to the subscriber by the service provider.
- **Demarcation (or demarc):** The juncture at which the CPE ends and the local loop portion of the service begins. It often occurs at a telecommunication closet.
- **Local loop (or “last-mile”):** Cabling (usually copper wiring) that extends from the demarcation point into the WAN service provider central office (CO).
- **CO switch:** A switching facility that provides the nearest point of presence (POP) for the provider WAN service. Inside the long-distance toll network are several types of COs.
- **Toll network:** The collective switches and facilities (called trunks) of the WAN provider. The call may cross a trunk to a primary center and then go to a sectional center and then to a regional or international carrier center as the call travels the long distance to its destination. Switches operate in provider offices, with toll charges based on tariffs or authorized rates.

# WAN Cabling

Cisco routers support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 standards for serial connections. This topic describes the cabling available for WAN connections.



To make a synchronous serial leased-line or packet-switched WAN connection, such as a Frame Relay connection, Cisco devices support the following serial standards:

- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA/TIA-530

When you order the cable, you will receive a shielded serial transition cable that has the appropriate connector for the standard that you specify. The router end of the shielded serial transition cable has a DB-60 connector, which connects to the DB-60 port on a serial WAN interface card (WIC). Because five different cable types are supported with this port, it is sometimes called a “5-in-1” serial port. The other end of the serial transition cable is available with the connector that is appropriate for the standard you specify. The documentation for the device to which you want to connect should indicate the standard used for that device.

Your CPE, in this case a router, is the data terminal equipment (DTE). The data circuit-terminating equipment (DCE), commonly a modem or channel service unit (CSU) and/or data service unit (DSU), is the device that is used to convert the user data from the DTE into a form acceptable to the WAN service provider. The synchronous serial port on the router is configured as DTE or DCE (except EIA/TIA-530, which is DTE only), depending on the attached cable, which is ordered as either DTE or DCE to match the router configuration. If the



port is configured as DTE (the default setting), it will require external clocking from the CSU/DSU or other DCE device.

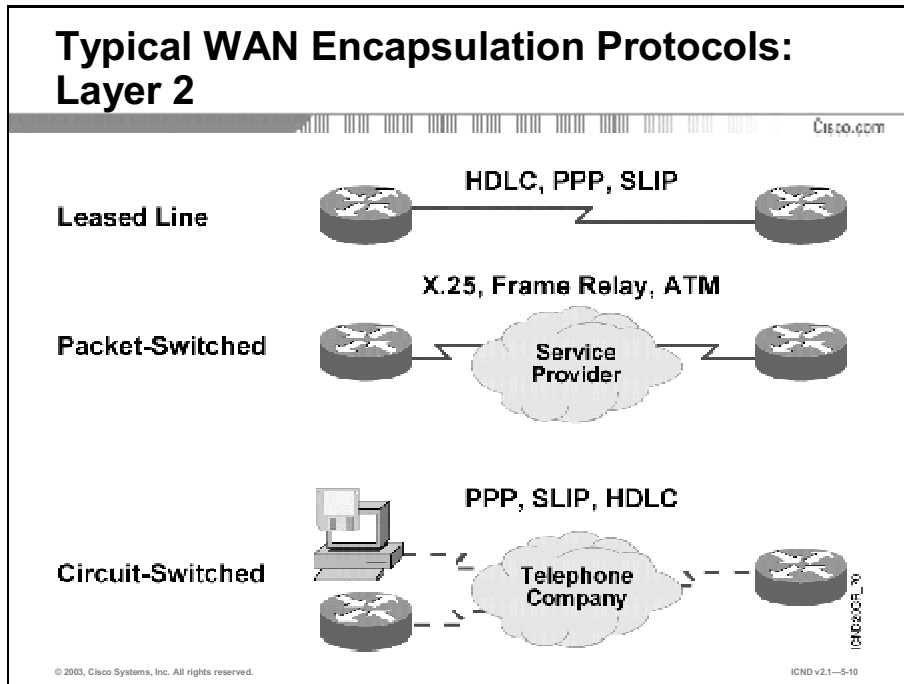
---

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | To support higher densities in a smaller form factor, Cisco has introduced a smart serial cable. The serial end of the smart serial cable is a 26-pin connector that is much smaller than the DB-60 connector used to connect to a five-in-one serial port. These transition cables support the same five serial standards, are available in either DTE or DCE configuration, and are used with the two-port serial and two-port asynchronous and/or synchronous WICs. |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

# Layer 2 Encapsulation Protocols

To encapsulate data for crossing a WAN link, you can choose from a variety of Layer 2 protocols, including High-Level Data Link Control (HDLC), PPP, Serial Line Internet Protocol (SLIP), X.25 and/or Link Access Procedure, Balanced (LAPB), Frame Relay, and ATM. This topic describes the different encapsulation protocols.



On each WAN connection, data is encapsulated into frames before crossing the WAN link. To ensure that the correct protocol is used, you will need to configure the appropriate Layer 2 encapsulation type. The choice of protocol depends on the WAN technology and the communicating equipment. Typical WAN protocols include the following:

- **HDLC:** The Cisco default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections. It is used typically when communicating between two Cisco devices. It is a bit-oriented synchronous data-link layer protocol. (HDLC is covered in more detail later in this lesson.)
- **PPP:** Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP was designed to work with several network-layer protocols, such as IP. PPP also has built-in security mechanisms such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- **SLIP:** A standard protocol for point-to-point serial connections using TCP/IP. SLIP has been largely replaced by PPP.
- **X.25 and/or LAPB:** International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard that defines how connections between a DTE and DCE are maintained for remote terminal access and computer communications in public data networks. X.25 specifies LAPB, a data-link layer protocol that manages the communication between DTE and DCE, including packet framing, ordering, and error checking. X.25 is a predecessor to Frame Relay.

- **Frame Relay:** Industry standard, switched data-link layer protocol that handles multiple VCs. It is a successor to X.25 that is streamlined to eliminate some of the time-consuming processes (such as error correction and flow control) that were employed in X.25 to compensate for older, less-reliable communication links.
- **ATM:** The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. ATM, a cell-switched technology, uses fixed-length cells, which allow processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as T3, E3, and SONET.

---

**Note**            SLIP, X.25, and ATM are not covered further here.

---

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary



- **A WAN makes data connections across a broad geographic area so that information can be exchanged between distant sites.**
- **Some of the WAN connection types available are leased line, circuit-switched, and packet-switched.**
- **Cisco routers support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 standards for serial connections.**
- **To encapsulate data for crossing a WAN link, you can choose from a variety of Layer 2 protocols, including HDLC, PPP, SLIP, X.25/LAPB, Frame Relay, and ATM.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—5-11

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) The primary difference between a WAN and a LAN is \_\_\_\_.
- A) size
  - B) cost
  - C) distance
  - D) reliability
- Q2) Which statement best describes a LAN?
- A) LANs are expensive to build.
  - B) LANs connect devices in a large geographic area.
  - C) LANs connect devices in a small geographic area.
  - D) LANs are generally leased from service providers.
- Q3) Which connection type is typically asynchronous?
- A) leased-line
  - B) point-to-point
  - C) circuit-switched
  - D) packet-switched
- Q4) Which term describes the cabling from a customer site into the service provider office?
- A) CO
  - B) CPE
  - C) demarc
  - D) local loop
- Q5) Which component provides clocking for a serial connection?
- A) DTE
  - B) DCE
  - C) V.35
  - D) DB-60

- Q6) Into which port does the router end of a transition cable connect?
- A) any DB-60 port
  - B) DB-60 port on a serial WIC
  - C) DB-60 port on a Fast Ethernet interface card
  - D) DB-60 port on a Gigabit Ethernet interface card
- Q7) Which Layer 2 encapsulation protocol has largely displaced SLIP for router-to-router and host-to-network connections?
- A) PPP
  - B) X.25
  - C) ATM
  - D) HDLC
- Q8) Which protocol is the Cisco default for dedicated serial links?
- A) PPP
  - B) X.25
  - C) ATM
  - D) HDLC

## Quiz Answer Key

- Q1) C  
**Relates to:** WAN Review
- Q2) C  
**Relates to:** WAN Review
- Q3) C  
**Relates to:** WAN Connection Types
- Q4) D  
**Relates to:** WAN Connection Types
- Q5) B  
**Relates to:** WAN Cabling
- Q6) B  
**Relates to:** WAN Cabling
- Q7) A  
**Relates to:** Layer 2 Encapsulation Protocols
- Q8) D  
**Relates to:** Layer 2 Encapsulation Protocols





# Configuring Serial Point-to-Point Encapsulation

---

## Overview

Serial point-to-point connections can be used to connect your LAN to your service provider WAN. This lesson describes the protocols used to encapsulate both data-link layer and network layer information over serial links and how to configure them.

## Relevance

You will most likely have serial point-to-point connections within your network and/or between your network and a service provider. You should know how to configure the serial ports for such connections.

## Objectives

Upon completing this lesson, you will be able to:

- Use Cisco IOS commands to configure serial interfaces using High-Level Data Link Control and PPP encapsulation for leased-line connections, given a functioning router
- Use **show** commands to identify anomalies in High-Level Data Link Control and PPP encapsulation for leased-line connections, given an operational router
- Use **debug** commands to identify events and anomalies in PPP configuration for leased-line connections, given an operational router

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

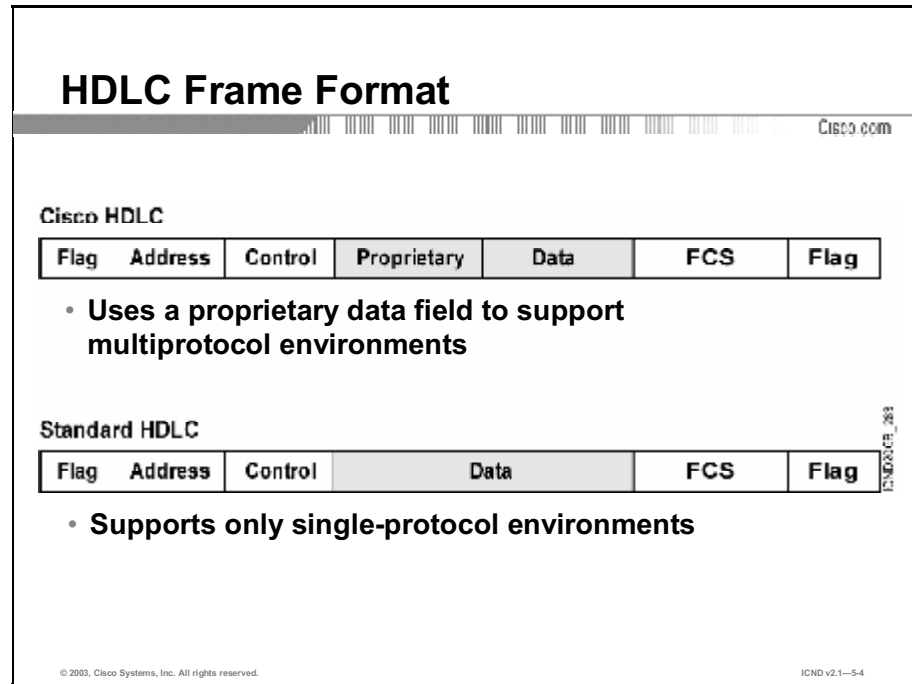
## Outline

The lesson includes these topics:

- Overview
- Configuring HDLC Encapsulation
- PPP Layered Architecture
- Configuring PPP
- Establishing a PPP Session
- PPP Authentication Protocols
- Configuring PPP Authentication
- Verifying the Serial Encapsulation Configuration
- Troubleshooting the PPP Authentication Configuration
- Summary
- Quiz

# Configuring HDLC Encapsulation

High-Level Data Link Control (HDLC) is the Cisco Systems default data-link layer protocol for encapsulating data on synchronous serial data links. This topic describes HDLC and explains how to reenabling the protocol on a serial port.



HDLC is an International Organization for Standardization (ISO) standard bit-oriented data-link layer protocol that encapsulates data on synchronous serial data links. Standard HDLC does not inherently support multiple protocols on a single link because it does not have a way to indicate which protocol it is carrying. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Cisco offers a proprietary version of HDLC. The Cisco HDLC frame uses a proprietary type field that acts as a protocol field, which makes it possible for multiple network layer protocols to share the same serial link.

---

**Note** HDLC does not provide link authentication.

---

# Configuring HDLC Encapsulation

Cisco.com

```
Router(config-if)#encapsulation hdlc
```

- Enables HDLC encapsulation
- Uses the default encapsulation on synchronous serial interfaces

© 2003, Cisco Systems, Inc. All rights reserved.

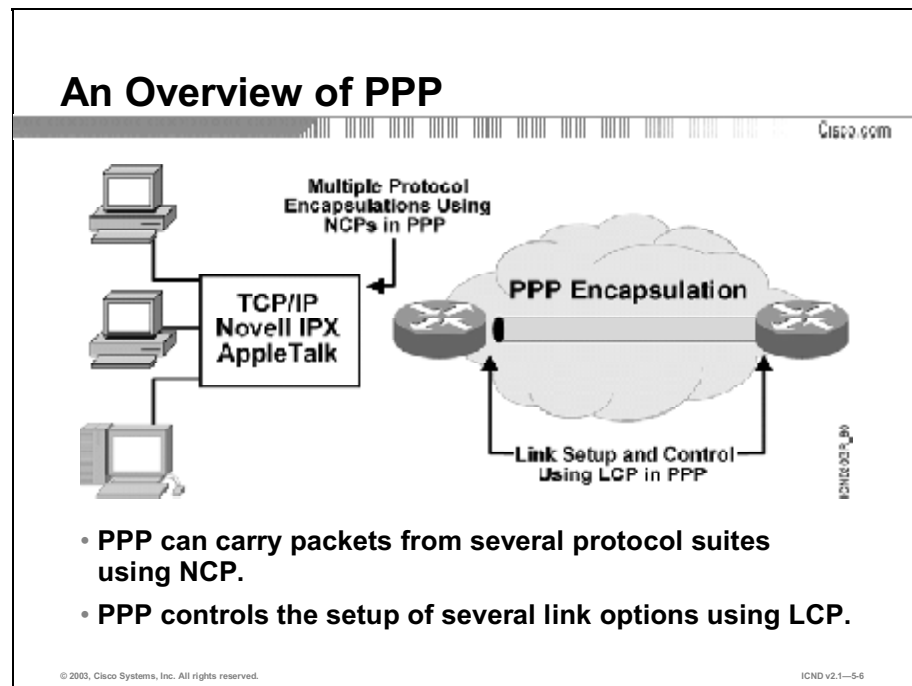
ICND v2.1—5-5

By default, Cisco devices use the Cisco HDLC serial encapsulation method on synchronous serial lines. However, if the serial interface is configured with another encapsulation protocol, and you want to change the encapsulation back to HDLC, enter the interface configuration mode of the interface that you wish to change. Enter the **encapsulation hdlc** interface configuration command to specify HDLC encapsulation on the interface.

Cisco HDLC is a PPP that can be used on leased lines between two Cisco devices. When communicating with a device from another vendor, synchronous PPP is a more viable option.

# PPP Layered Architecture

PPP encapsulates network layer protocol information over point-to-point links. This topic describes the PPP layered architecture.



Developers on the Internet designed PPP to make the connection for point-to-point links. PPP, described in RFCs 1661 and 1332, encapsulates network layer protocol information over point-to-point links. RFC 1661 is updated by RFC 2153, *PPP Vendor Extensions*.

You can configure PPP on the following types of physical interfaces:

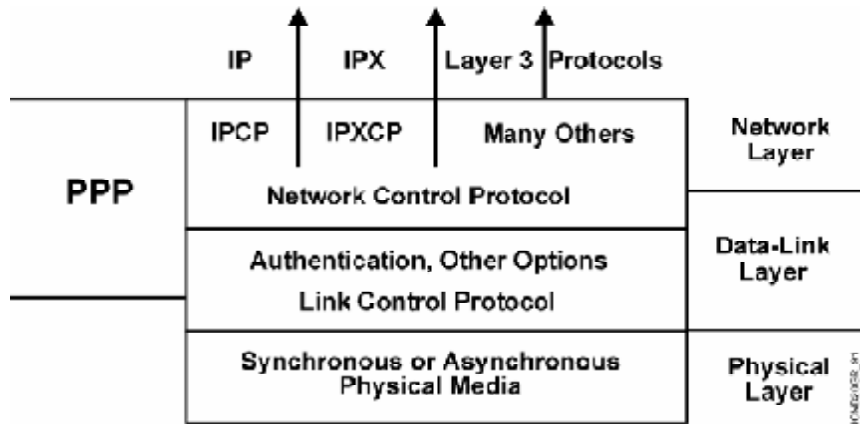
- Asynchronous serial
- Synchronous serial
- High-Speed Serial Interface (HSSI)
- ISDN

PPP uses its Network Control Program (NCP) component to encapsulate and negotiate options for multiple network layer protocols.

PPP uses another of its major components, the link control protocol (LCP), to negotiate and set up control options on the WAN data link.

## Layering PPP Elements

Cisco.com



• **PPP—a data link with network layer services**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-7

PPP uses a layered architecture. With its lower-level functions, PPP can use the following:

- Synchronous physical media
- Asynchronous physical media like those that use basic telephone service for modem dialup connections
- ISDN

PPP offers a rich set of services that control the setup of a data link. These services are options in LCP and are primarily negotiation and checking frame options to implement the point-to-point controls that an administrator specifies for the call.

With its higher-level functions, PPP carries packets from several network layer protocols using NCPs. These include functional fields containing standardized codes to indicate the network layer protocol type that PPP encapsulates.

# Configuring PPP

Configurable aspects of PPP include methods of authentication, compression, and error detection, as well as whether or not multilink is supported. This topic describes the different configuration options for PPP.

| PPP LCP Configuration Options |                                                              |                            |
|-------------------------------|--------------------------------------------------------------|----------------------------|
| Feature                       | How It Operates                                              | Protocol                   |
| Authentication                | Requires a password<br>Performs challenge handshake          | PAP<br>CHAP                |
| Compression                   | Compresses data at source;<br>reproduces data at destination | Stacker or<br>Predictor    |
| Error Detection               | Monitors data dropped on link<br>Avoids frame looping        | Quality<br>Magic Number    |
| Multilink                     | Load-balances across<br>multiple links                       | Multilink<br>Protocol (MP) |

RFC 1548 describes PPP operation and link control protocol (LCP) configuration options. RFC 1548 is updated by RFC 1570, *PPP LCP Extensions*.

Cisco routers that use PPP encapsulation may include these LCP configuration options, shown in the figure:

- Authentication options require that the calling side of the link enters information to help ensure that the caller has the network administrator permission to make the call. Peer routers exchange authentication messages. Two alternatives are as follows:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- Compression options increase the effective throughput on PPP connections by reducing the amount of data in the original frame that must travel across the link. The protocol decompresses the frame at its destination.

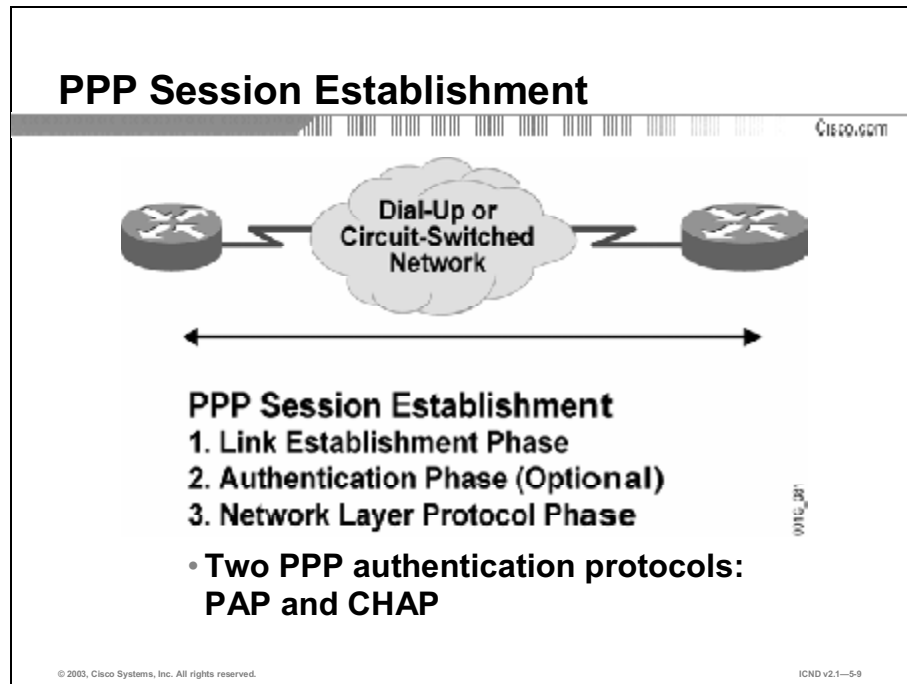
Two compression protocols available in Cisco routers are Stacker and Predictor.

- Error-detection mechanisms with PPP enable a process to identify fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link.
- Cisco IOS Release 11.1 (and later releases), support Multilink Protocol (MP). This feature is sometimes referred to as Multilink PPP (MLP). This alternative provides load balancing over the router interfaces that PPP uses.

MP, as specified in RFC 1717, provides packet fragmentation and sequencing that splits the load for PPP and sends fragments over parallel circuits. In some cases, this “bundle” of MLP pipes functions as a single logical link, improving throughput and reducing latency between peer routers. RFC 1990, *The PPP Multilink Protocol (MP)*, obsoletes RFC 1717.

# Establishing a PPP Session

PPP session establishment progresses through three phases: link establishment, authentication, and network layer protocol. This topic describes the three phases of PPP session establishment.



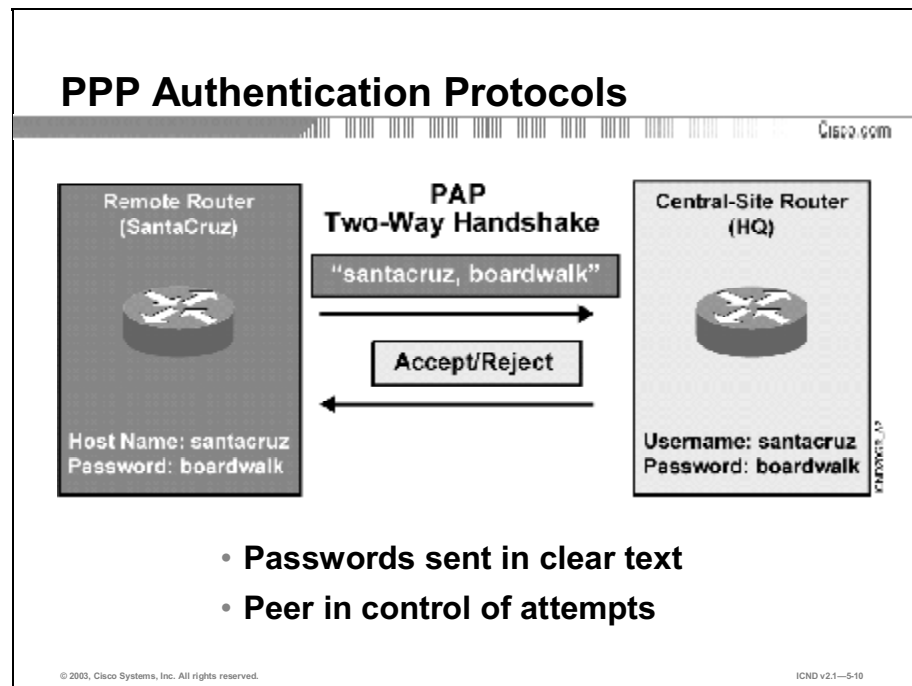
A PPP session establishment has three phases, as follows:

| Phase | Authentication Phase            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.    | Link establishment phase        | In this phase, each PPP device sends LCP packets to configure and test the data link. LCP packets contain a Configuration Option field that allows devices to negotiate the use of options, such as the maximum receive unit, compression of certain PPP fields, and the link authentication protocol. If a configuration option is not included in an LCP packet, the default value for that configuration option is assumed.                                               |
| 2.    | Authentication phase (optional) | <p>After the link has been established, and the authentication protocol decided on, the peer may be authenticated. Authentication, if used, takes place <i>before</i> the network layer protocol phase is entered.</p> <p>PPP supports two authentication protocols: PAP and CHAP. Both of these protocols are detailed in RFC 1334, <i>PPP Authentication Protocols</i>. However, RFC 1994, <i>PPP Challenge Handshake Authentication Protocol</i>, obsoletes RFC 1334.</p> |
| 3.    | Network layer protocol phase    | In this phase, the PPP devices send NCP packets to choose and configure one or more network layer protocols, such as IP. After each of the chosen network layer protocols have been configured, datagrams from each network layer protocol can be sent over the link.                                                                                                                                                                                                        |



# PPP Authentication Protocols

When configuring PPP authentication, you can select PAP or CHAP. In general, CHAP is the preferred protocol. This topic describes the two PPP authentication protocols.



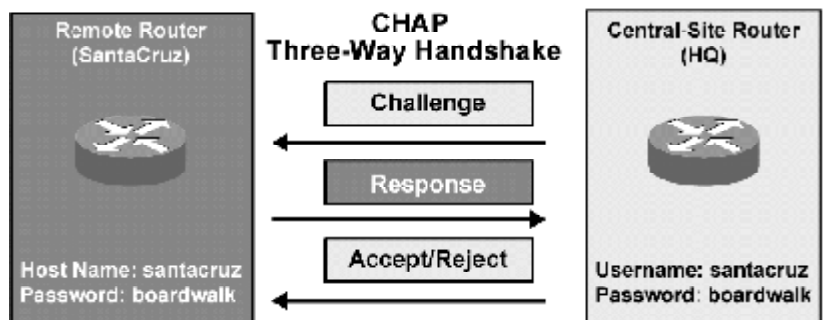
PAP provides a simple method for a remote node to establish its identity using a two-way handshake. PAP is done only upon initial link establishment.

After the PPP link establishment phase is complete, a username and password pair are repeatedly sent by the remote node to the router until authentication is acknowledged or the connection is terminated.

PAP is not a strong authentication protocol. Passwords are sent across the link in clear text and there is no protection from playback or repeated trial-and-error attacks. The remote node is in control of the frequency and timing of the login attempts. A clear text password, however, may be fine in environments that use token-type passwords that change with each authentication.

# Challenge Handshake Authentication Protocol

Cisco.com



- Hash values, not actual passwords, are sent across link.
- The local router or external server is in control of attempts.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-11

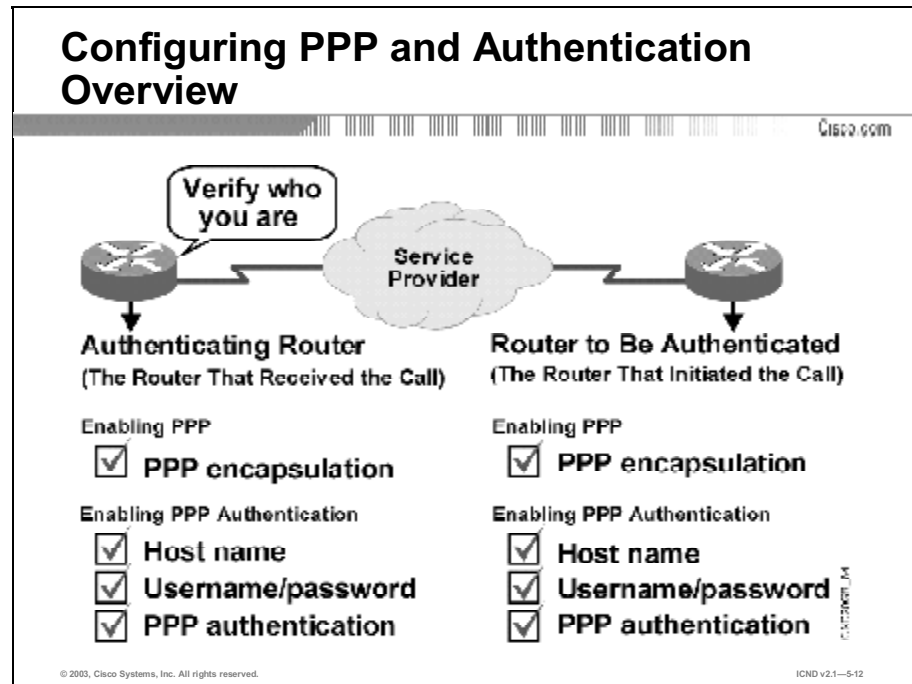
CHAP is used at the startup of a link and periodically to verify the identity of the remote node using a three-way handshake. CHAP is done upon initial link establishment and can be repeated anytime after the link has been established.

After the PPP link establishment phase is complete, the local router sends a “challenge” message to the remote node. The remote node responds with a value that is calculated using a one-way hash function (typically Message Digest 5, or MD5) based on the password and challenge message. The local router checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value will also be unique and random. The use of repeated challenges is intended to limit the time of exposure to any single attack. The local router or a third-party authentication server is in control of the frequency and timing of the challenges.

# Configuring PPP Authentication

You enable PPP with the **encapsulation ppp** command and PPP authentication with the **ppp authentication** command. This topic describes how to configure PPP authentication.



To enable PPP encapsulation and PAP or CHAP authentication on an interface, complete the checklist indicated in the figure.

## Configuring PPP

Cisco.com

```
Router(config-if)#encapsulation ppp
```

- **Enables PPP encapsulation**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-13

To enable PPP encapsulation, enter interface configuration mode. Enter the **encapsulation ppp** interface configuration command to specify PPP encapsulation on the interface.

---

|             |                                                                                                                                                                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Additional configuration steps are required to enable PPP on an asynchronous serial interface. These steps are not taught in this course. For additional information about configuring PPP on an asynchronous serial interface, refer to the <i>Building Cisco Remote Access Networks</i> (BCRAN) course. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

# Configuring PPP Authentication

Cisco.com

```
Router(config)#hostname name
```

- Assigns a host name to your router

```
Router(config)#username name password password
```

- Identifies the username and password of remote router

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-14

To configure PPP authentication, the interface must be configured for PPP encapsulation. Enable PAP or CHAP authentication by performing the following steps:

1. Verify that each router has a host name assigned to it. To assign a host name, enter the **hostname** *name* command in global configuration mode. This name must match the username expected by the authenticating router at the other end of the link.
2. On each router, define the username and password to expect from the remote router with the **username** *name* **password** *password* global configuration command.

| username<br>Command Parameters | Description                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                    | This is the host name of the remote router. Note that it is case sensitive.                                                                                                                                                                                                                                                                                                        |
| <i>password</i>                | On Cisco routers, the password must be the same for both routers. In pre-Release 11.2 Cisco IOS software, this password was an encrypted, secret password. As of Release 11.2, the password is a plain-text password. It is not encrypted. To encrypt passwords on your Cisco IOS router, enter the <b>service password-encryption</b> command while in global configuration mode. |

Add a username entry for each remote system that the local router communicates with and that requires authentication. The remote device must also have a corresponding username entry for the local router with a matching password.

## Configuring PPP Authentication (Cont.)

Cisco.com

```
Router(config-if)#ppp authentication
{chap | chap pap | pap chap | pap}
```

- **Enables PAP and/or CHAP authentication**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-15

Configure PPP authentication with the **ppp authentication {chap | chap pap | pap chap | pap}** interface configuration command.

If you configure **ppp authentication chap** on an interface, all incoming calls on that interface that initiate a PPP connection will be authenticated using CHAP. Likewise, if you configure **ppp authentication pap**, all incoming calls that start a PPP connection will be authenticated using PAP.

If you configure **ppp authentication chap pap**, the router will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the router will try to authenticate the call using PAP. If the remote device does not support either CHAP or PAP, authentication will fail and the call will be dropped.

If you configure **ppp authentication pap chap**, the router will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device does not support either protocol, authentication will fail and the call will be dropped.

---

|             |                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | If both methods are enabled, then the first method specified will be requested during link negotiation. If the peer suggests using the second method or simply refuses the first method, then the second method will be tried. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## CHAP Configuration Example

Cisco.com



```
hostname left
username right password someone
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

```
hostname right
username left password someone
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-16

In the figure, a two-way challenge occurs. The host name on one router must match the username the other router has configured. The passwords must also match.

The following is an example of a two-way PAP authentication configuration. Both routers authenticate and are authenticated, so the PAP authentication commands mirror each other. The PAP username and password that each router sends must match those specified with the **username name password password** command of the other router:

```
hostname left
username right password cisco
!
interface serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication pap
```

```
hostname right
username left password cisco
!
interface serial 0
 ip address 10.0.1.2
 encapsulation ppp
 ppp authentication pap
```

# Verifying the Serial Encapsulation Configuration

Use the **show interface** command to verify proper configuration of HDLC or PPP encapsulation. This topic describes how to verify the HDLC and PPP configuration.

## Verifying the HDLC and PPP Encapsulation Configuration



```
Router#show interface s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:05, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 38021 packets input, 5656110 bytes, 0 no buffer
Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 38097 packets output, 2135697 bytes, 0 underruns
 0 output errors, 0 collisions, 6045 interface resets
 0 output buffer failures, 0 output buffers swapped out
482 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

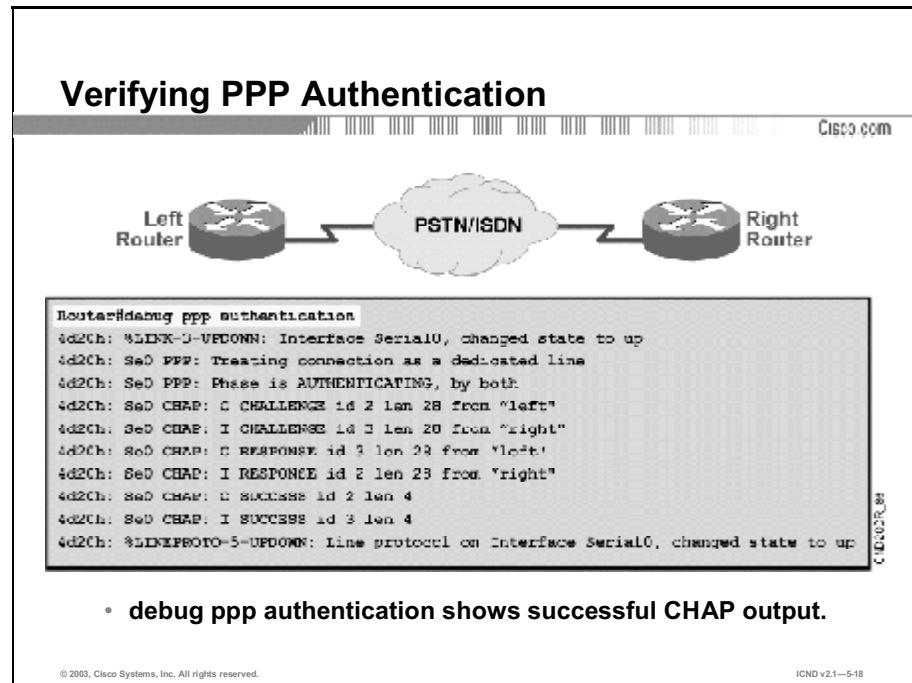
© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—5-17

Use the **show interface** command to verify proper configuration. The figure illustrates a PPP configuration. When HDLC is configured, “Encapsulation HDLC” should be reflected in the output of the **show interface** command. When PPP is configured, you can also check its LCP and NCP states using this command.



## Troubleshooting the PPP Authentication Configuration

The **debug ppp authentication** command displays the authentication exchange sequence. This topic describes how to use the **debug ppp authentication** command to troubleshoot PPP authentication.



The figure illustrates the left router output during CHAP authentication with the router on the right when **debug ppp authentication** is enabled. Because two-way authentication is configured, that is, each router authenticates the other, messages will appear for both the authenticating process and the process of being authenticated. Use this command to display the exchange sequence as it occurs.

The following output highlights the left router output for a two-way PAP authentication:

```
Se0 PPP: Phase is AUTHENTICATING, by both (Two way
authentication)
Se0 PAP: O AUTH-REQ id 4 len 18 from "left" (Outgoing
authentication request)
Se0 PAP: I AUTH-REQ id 1 len 18 from "right" (Incoming
authentication request)
Se0 PAP: Authenticating peer right (Authenticating
incoming)
Se0 PAP: O AUTH-ACK id 1 len 5 (Outgoing
acknowledgement)
Se0 PAP: I AUTH-ACK id 4 len 5 (Incoming
acknowledgement)
```

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **HDLC is the Cisco default data-link layer protocol for encapsulating data on synchronous serial data links.**
- **PPP encapsulates network layer protocol information over point-to-point links.**
- **Configurable aspects of PPP include methods of authentication, compression, and error detection, as well as whether or not multilink is supported.**
- **PPP session establishment progresses through three phases: link establishment, authentication, and network layer protocol.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-19

## Summary (Cont.)

Cisco.com

- **When configuring PPP authentication, you can select PAP or CHAP. In general, CHAP is the preferred protocol.**
- **You enable PPP with the encapsulation ppp command and PPP authentication with the ppp authentication command.**
- **Use the show interface command to verify proper configuration of PPP encapsulation.**
- **The debug ppp authentication command displays the authentication exchange sequence.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—5-20

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

## Next Steps

After completing this lesson, go to:

- Lab Exercise 5-1: Configuring Serial Connections to WAN Service Providers

# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which field in the Cisco-proprietary HDLC frame differs from the standard HDLC frame?
- A) flag
  - B) FCS
  - C) type
  - D) control
- Q2) In what mode of the Cisco command-line interface (CLI) do you use the **encapsulation** command?
- A) user mode
  - B) global configuration mode
  - C) interface configuration mode
  - D) subinterface configuration mode
- Q3) PPP uses \_\_\_\_\_ to negotiate and set up control options on the WAN data link.
- A) NCP
  - B) LCP
  - C) IPCP
  - D) IPXCP
- Q4) What is the purpose of NCP?
- A) to perform authentication
  - B) to negotiate control options
  - C) to encapsulate multiple protocols
  - D) to specify asynchronous vs. synchronous
- Q5) Which feature provides load balancing over the router interfaces that PPP uses?
- A) CHAP
  - B) predictor
  - C) compression
  - D) multilink PPP

- Q6) The Magic Number is used by LCP to provide which PPP feature?
- A) multilink
  - B) compression
  - C) authentication
  - D) error detection
- Q7) In which PPP session establishment phase is the authentication protocol negotiated?
- A) Authentication.
  - B) Link establishment.
  - C) Network layer protocol.
  - D) None, it is predetermined.
- Q8) The network layer protocol phase uses which type of packets?
- A) LCP
  - B) PAP
  - C) NCP
  - D) CHAP
- Q9) Which two statements best describe PAP? (Choose two.)
- A) PAP is performed periodically.
  - B) PAP uses a two-way handshake.
  - C) PAP uses a three-way handshake.
  - D) PAP uses a one-way hash function.
  - E) PAP passwords are sent in clear text.
- Q10) Which CHAP feature is intended to limit the time of exposure to replay attacks?
- A) repeated challenges
  - B) three-way handshake
  - C) one-way hash function
  - D) variable challenge values
- Q11) At what Cisco CLI mode do you enter the command to specify a user password?
- A) user mode
  - B) ROM monitor mode
  - C) global configuration mode
  - D) interface configuration mode

- Q12) In the command **username** *name* **password** *password*, what does *name* represent?
- A) the host name of the local router
  - B) the host name of the remote router
  - C) the name of a user on the local router
  - D) the name of a user on the remote router
- Q13) Which command do you use to verify proper PPP encapsulation configuration?
- A) **show ppp**
  - B) **show interface**
  - C) **show interface ppp**
  - D) **show running-config**
- Q14) How many messages are exchanged for two-way CHAP authentication?
- A) 4
  - B) 5
  - C) 6
  - D) 7

## Quiz Answer Key

- Q1) C  
**Relates to:** Configuring High-Level Data Link Control Encapsulation
- Q2) C  
**Relates to:** Configuring High-Level Data Link Control Encapsulation
- Q3) B  
**Relates to:** PPP Layered Architecture
- Q4) C  
**Relates to:** PPP Layered Architecture
- Q5) D  
**Relates to:** Configuring PPP
- Q6) D  
**Relates to:** Configuring PPP
- Q7) B  
**Relates to:** Establishing a PPP Session
- Q8) C  
**Relates to:** Establishing a PPP Session
- Q9) B, E  
**Relates to:** PPP Authentication Protocols
- Q10) A  
**Relates to:** PPP Authentication Protocols
- Q11) C  
**Relates to:** Configuring PPP Authentication
- Q12) B  
**Relates to:** Configuring PPP Authentication
- Q13) B  
**Relates to:** Troubleshooting the PPP Authentication Configuration
- Q14) C  
**Relates to:** Troubleshooting the PPP Authentication Configuration





# Lesson Assessments

---

## Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

## Outline

This section includes these assessments:

- Lesson Assessment 5-1: Wide-Area Networking Review
- Lesson Assessment 5-2: Configuring Serial Point-to-Point Encapsulation

# Lesson Assessment 5-1: Wide-Area Networking Review

Complete this quiz to assess what you learned in the lesson.

## Objectives

This quiz tests your knowledge of how to:

- Describe leased-line, circuit-switched, and packet-switched networks
- Define terms used by WAN service providers, including customer premises equipment demarcation, local loop, central office, and toll network
- Identify the five serial standards supported by Cisco devices
- Describe the major WAN protocols including High-Level Data Link Control, PPP, Serial Line Internet Protocol, X.25, Frame Relay, and ATM

## Quiz

Answer these questions:

- Q1) Which two features describe a WAN? (Choose two.)
- A) low cost
  - B) generally built in-house
  - C) generally leased from service providers
  - D) connects devices in a small geographic area
  - E) connects sites across a large geographic area
- Q2) Which two connection types are typically synchronous? (Choose two.)
- A) telephone
  - B) leased-line
  - C) circuit-switched
  - D) packet-switched
- Q3) Which two WAN connection types use virtual circuits? (Choose two.)
- A) leased-line
  - B) cell-switched
  - C) circuit-switched
  - D) packet-switched
- Q4) A demarcation marks the juncture between what other two WAN components? (Choose two.)
- A) trunk
  - B) CPE
  - C) local loop
  - D) CO switch
  - E) toll network

- Q5) Which type of serial transition cable should you select to connect a Cisco router to a CSU/DSU with a V.35 connection?
- A) V.35
  - B) DB-60
  - C) V.35-DTE
  - D) V.35-DCE
- Q6) The synchronous serial port is configured as \_\_\_\_\_ or \_\_\_\_\_, depending on the attached cable.
- A) DTE, CO
  - B) CPE, DTE
  - C) DTE, DCE
  - D) CPE, DCE
- Q7) PPP has largely displaced which Layer 2 encapsulation protocol?
- A) X.25
  - B) ATM
  - C) SLIP
  - D) HDLC
- Q8) Which WAN protocol uses fixed-length cells?
- A) PPP
  - B) X.25
  - C) ATM
  - D) HDLC
- Q9) Frame Relay is the successor to which WAN protocol?
- A) PPP
  - B) X.25
  - C) ATM
  - D) HDLC
- Q10) Which WAN protocol is the default encapsulation typically implemented between two Cisco devices?
- A) PPP
  - B) X.25
  - C) ATM
  - D) HDLC

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment 5-2: Configuring Serial Point-to-Point Encapsulation

Complete this quiz to assess what you learned in the lesson.

## Objectives

This quiz tests your knowledge of how to:

- Use Cisco IOS commands to configure serial interfaces using High-Level Data Link Control and PPP encapsulation for leased-line connections, given a functioning router
- Use **show** commands to identify anomalies in High-Level Data Link Control and PPP encapsulation for leased-line connections, given an operational router
- Use **debug** commands to identify events and anomalies in PPP configuration for leased-line connections, given an operational router

## Quiz

Answer these questions:

- Q1) Which command enables HDLC?
- A) **Router (config)# hdlc encapsulation**
  - B) **Router (config)# encapsulation hdlc**
  - C) **Router (config-if)# hdlc encapsulation**
  - D) **Router (config-if)# encapsulation hdlc**
- Q2) How does the Cisco-proprietary HDLC make it possible for multiple network-layer protocols to share the same serial link?
- A) It adds a new type field.
  - B) It subdivides the control field.
  - C) It provides for additional values in the FCS field.
  - D) It includes protocol information with the data field.
- Q3) What feature does PPP use to encapsulate multiple protocols?
- A) NCP
  - B) LCP
  - C) IPCP
  - D) IPXCP
- Q4) What is the purpose of LCP?
- A) to perform authentication
  - B) to negotiate control options
  - C) to encapsulate multiple protocols
  - D) to specify asynchronous vs. synchronous

- Q5) Stacker is a protocol for which PPP feature?
- A) multilink
  - B) compression
  - C) authentication
  - D) error detection
- Q6) In which PPP session establishment phase is the maximum receive unit size negotiated?
- A) authentication
  - B) link establishment
  - C) network layer protocol
  - D) none, it is predetermined
- Q7) Which packet types are used in the PPP link establishment phase?
- A) LCP
  - B) PAP
  - C) NCP
  - D) CHAP
- Q8) Which feature increases the effective throughput on PPP links?
- A) CHAP
  - B) compression
  - C) authentication
  - D) Multilink PPP
- Q9) Which two statements best describe CHAP? (Choose two.)
- A) CHAP is performed periodically.
  - B) CHAP uses a two-way handshake.
  - C) CHAP uses a three-way handshake.
  - D) CHAP uses a two-way hash function.
  - E) CHAP passwords are sent in clear text.
- Q10) When is PAP authentication performed?
- A) periodically
  - B) on user command
  - C) at link establishment
  - D) at link establishment, and then periodically thereafter
- Q11) With CHAP, how does a remote node respond to a challenge message?
- A) with a hash value
  - B) with a return challenge
  - C) with a clear text password
  - D) with an encrypted password

- Q12) Which setting must be the same on both Cisco routers involved in PPP authentication?
- A) nothing
  - B) the password
  - C) the username
  - D) the host name
- Q13) Which username must be configured on routers for PPP authentication?
- A) One that matches neither host name.
  - B) There is no restriction on username.
  - C) One that matches the host name of the local router.
  - D) One that matches the host name of the remote router.
- Q14) In what Cisco CLI mode do you enter the command to specify PPP authentication?
- A) user mode
  - B) ROM monitor mode
  - C) global configuration mode
  - D) interface configuration mode
- Q15) What does the **ppp authentication chap pap** command configure?
- A) CHAP authentication will always be used.
  - B) Either CHAP or PAP will be used, selected at random for security.
  - C) CHAP authentication will be used unless the remote router requests PAP.
  - D) If authentication fails using CHAP, then PAP authentication is attempted.
- Q16) Which output from the **show interface** command indicates that PPP is configured properly?
- A) encaps=PPP
  - B) PPP encapsulation
  - C) Encapsulation PPP
  - D) Encapsulation HDLC using PPP
- Q17) Which statement may appear in the output of the **debug ppp authentication** command for CHAP authentication?
- A) O AUTH-ACK id 1 len 5
  - B) O AUTH-REQ id 4 len 18 from "left"
  - C) I AUTH-REQ id 1 len 18 from "right"
  - D) O CHALLENGE id 2 len 28 from "left"
- Q18) How many messages are exchanged for two-way PAP authentication?
- A) 4
  - B) 5
  - C) 6
  - D) 7

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment Answer Key

## Lesson Assessment 5-1: Wide-Area Networking Review

- Q1) C, E
- Q2) B, D
- Q3) B, D
- Q4) B, C
- Q5) C
- Q6) C
- Q7) C
- Q8) C
- Q9) B
- Q10) D

## Lesson Assessment 5-2: Configuring Serial Point-to-Point Encapsulation

- Q1) D
- Q2) A
- Q3) A
- Q4) B
- Q5) B
- Q6) B
- Q7) A
- Q8) B
- Q9) A, C
- Q10) C
- Q11) A
- Q12) B
- Q13) D
- Q14) D
- Q15) C
- Q16) C
- Q17) D
- Q18) C





# Establishing Frame Relay Connections

---

## Overview

Frame Relay is a high-performance WAN protocol that operates at the physical and data-link layers of the OSI reference model. Internationally, Frame Relay was standardized by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). In the United States, Frame Relay is an American National Standards Institute (ANSI) standard. This module describes Frame Relay operation and shows you how to configure Frame Relay on Cisco Systems routers.

Upon completing this module, you will be able to:

- Use Cisco IOS commands to configure an operational serial Frame Relay connection and Frame Relay subinterfaces, given a functioning router
- Use **show** commands to identify anomalies in an operational serial Frame Relay connection and Frame Relay subinterfaces, given a functioning router
- Use **debug** commands to identify events and anomalies in an operational serial Frame Relay connection and Frame Relay subinterfaces, given a functioning router and an operational serial Frame Relay connection

## Outline

The module contains these lessons:

- Frame Relay Overview
- Configuring Frame Relay
- Lesson Assessments



# Frame Relay Overview

---

## Overview

Frame Relay is a high-performance WAN protocol that operates at the physical and data-link layers of the Open System Interconnection (OSI) reference model. Internationally, Frame Relay was standardized by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). In the United States, Frame Relay is an American National Standards Institute (ANSI) standard. This module describes Frame Relay operation.

## Relevance

Frame Relay is a key WAN service implemented at many institutions. Understanding Frame Relay operation is important before you configure its services.

## Objectives

Upon completing this lesson, you will be able to:

- Describe the features and operation of a Frame Relay network
- Define important Frame Relay terms, including local access rate, virtual circuit, permanent virtual circuit, switched virtual circuit, data-link connection identifier, committed information rate, Inverse Address Resolution Protocol, Local Management Interface, forward explicit congestion notification, and backward explicit congestion notification

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

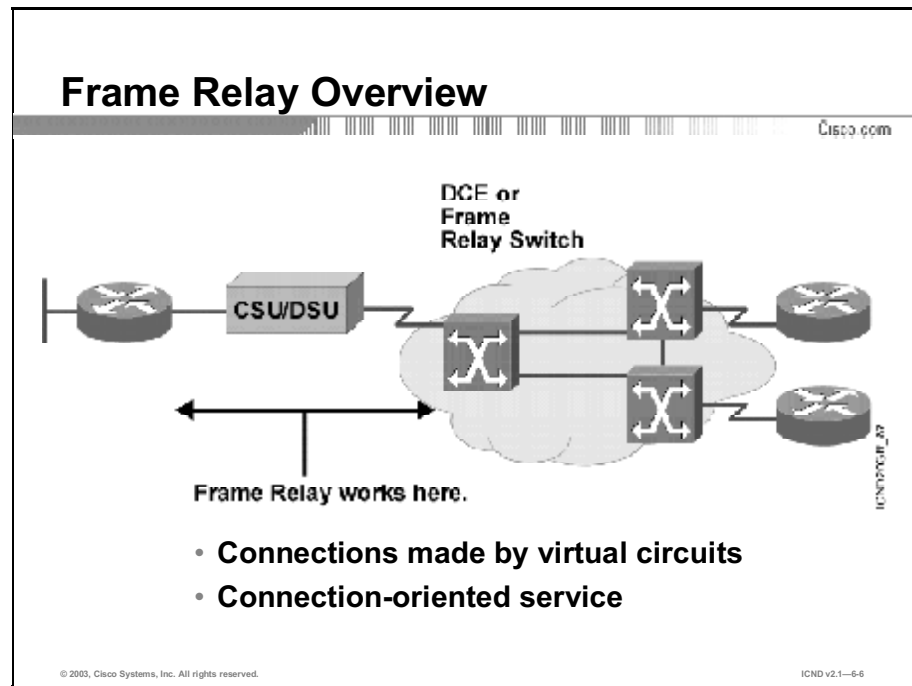
# Outline

This lesson includes these topics:

- Overview
- Introducing Frame Relay
- Frame Relay Stack Layered Support
- Frame Relay Terminology
- Frame Relay Topologies
- Resolving Reachability Issues in Frame Relay
- Frame Relay Address Mapping
- Frame Relay Signaling
- How Service Providers Map Frame Relay Data-Link Connection Identifiers
- Service Provider Frame Relay-to-ATM Interworking
- Summary
- Quiz

# Introducing Frame Relay

Frame Relay provides connection-oriented data-link layer communication. Frame Relay uses virtual circuit (VC), which is a logical connection created between two data terminal equipment (DTE) devices across the Frame Relay service provider network. This topic introduces the basic functionality provided by Frame Relay.



Frame Relay is a connection-oriented data-link technology that is streamlined to provide high performance and efficiency. It relies on upper-layer protocols for error correction and the more dependable fiber and digital networks of today.

Frame Relay defines the interconnection process between the router and the service provider local access switching equipment. It does *not* define how the data is transmitted within the Frame Relay service provider “cloud.”

Devices attached to a Frame Relay WAN fall into two general categories: DTE and data circuit-terminating equipment (DCE).

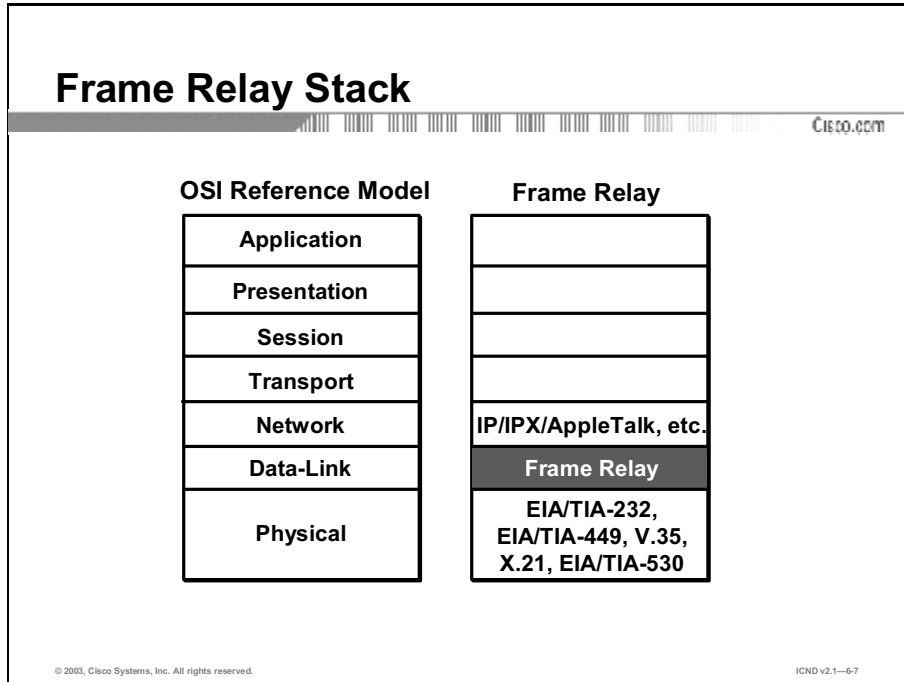
DTEs are generally considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are Frame Relay access devices (FRADs), routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network and transmit data through the WAN. In most cases, these are the Frame Relay switches.

Frame Relay provides a means for statistically multiplexing many logical data conversations (referred to as VCs) over a single physical transmission link by assigning connection identifiers to each pair of DTEs. The service provider switching equipment constructs a switching table, mapping the connection identifier to outbound ports. When a frame is received, the switching device analyzes the connection identifier and delivers the frame to the associated outbound port. The complete path to the destination is established *prior* to the transmission of the first frame.

# Frame Relay Stack Layered Support

The core aspects of Frame Relay function at the lower two layers of the Open System Interconnection (OSI) reference model. This topic describes the operation of the core aspects of Frame Relay within the OSI reference model.



The same physical serial connections that support point-to-point environments also support the Frame Relay connection to the service provider. Cisco routers support the following serial connections:

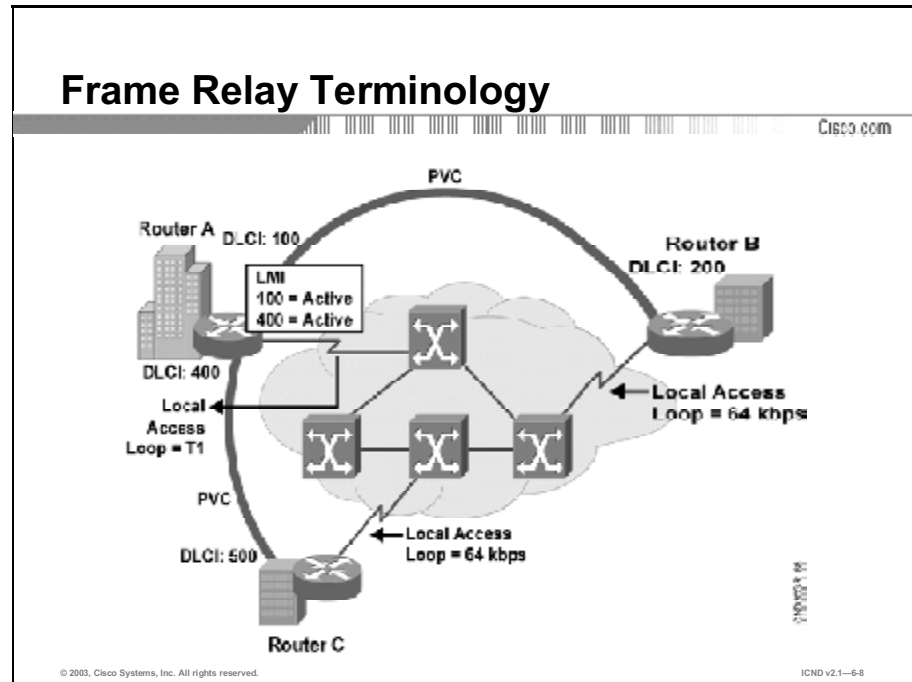
- EIA/TIA-232
- EIA/TIA-449
- V.35
- X.21
- EIA/TIA-530

Working at the data-link layer, Frame Relay encapsulates information from the upper layers of the OSI model. For example, IP traffic would be encapsulated into a frame format that can be transmitted over a Frame Relay link.

A Frame Relay frame contains the following fields: opening flag (0x7E), address, data, frame check sequence (FCS), and closing flags (0x7E). The address field, which is two bytes in length, is comprised of 10 bits representing the actual circuit identifier and six bits of fields related to congestion management. The data field contains encapsulated upper-layer data.

# Frame Relay Terminology

Knowing the terms that are used frequently when discussing Frame Relay is important in understanding the operation and configuration of Frame Relay services. This topic describes the key Frame Relay terms.



The following are some terms that are used frequently when discussing Frame Relay:

- **Local access rate:** The clock speed (port speed) of the connection (local loop) to the Frame Relay cloud. It is the rate at which data travels into or out of the network, regardless of other settings.
- **VC:** Logical circuits that are created to ensure bidirectional communication from one DTE device to another, and uniquely identified by a data-link connection identifier (DLCI). A number of VCs can be multiplexed into a single physical circuit for transmission across the network. This capability often can reduce the equipment and network complexity required to connect multiple DTE devices. A VC can pass through any number of intermediate DCE devices (Frame Relay switches). A VC can be either a permanent virtual circuit (PVC) or a switched virtual circuit (SVC).
- **PVC:** Permanently established connections that are used for frequent and consistent data transfers between DTE devices across the Frame Relay network. Communication across a PVC does not require the call setup and call teardown used with SVCs.
- **SVC:** Temporary connections that are used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. SVCs are dynamically established on demand and are torn down when transmission is complete.

---

**Note** With American National Standards Institute (ANSI) T1.617, ITU-T Q.933 (Layer 3), and Q.922 (Layer 2), Frame Relay now supports SVCs. Cisco IOS Release 11.2 or later supports Frame Relay SVCs. Information on configuring Frame Relay SVCs is not covered in this course.

---

- **DLCI:** A 10-bit number in the address field of the Frame Relay frame header that identifies the VC. DLCIs have local significance because the identifier references the point between the local router and the local Frame Relay switch to which it is connected. Therefore, devices at opposite ends of a connection can use different DLCI values to refer to the same virtual connection.

For example, as shown in the figure, router A has two VCs configured on the physical interface. A DLCI of 100 identifies the VC that connects to router B. A DLCI of 400 identifies the VC that connects to router C. At the other end, a different DLCI number can be used to identify the VC.

- **Committed information rate (CIR):** When subscribing to Frame Relay service, you will specify the local access rate (for example, 56 kbps or T1) and also, typically, you will be asked to specify a CIR for each DLCI. The CIR value specifies the maximum average data rate that the network undertakes to deliver under “normal conditions.” If you send faster than the CIR on a given DLCI, the network will flag some frames with a discard eligible (DE) bit. The network will do its best to deliver all packets but will discard any DE packets first if there is congestion. Many inexpensive Frame Relay services are based on a CIR of zero. This means that every frame is a DE frame, and the network will throw any frame away when it needs to. The DE bit is within the address field of the Frame Relay frame header.
- **Inverse Address Resolution Protocol (Inverse ARP):** Method of dynamically associating the remote router network layer address with a local DLCI. It allows a router to automatically discover the network address of the remote DTE device associated with a VC.
- **Local Management Interface (LMI):** A signaling standard between the router (DTE device) and the local Frame Relay switch (DCE device) that is responsible for managing the connection and maintaining status between the router and the Frame Relay switch.
- **Forward explicit congestion notification (FECN):** The FECN bit is a bit in the address field of the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (Frame Relay switches) set the FECN bit value of the frames to one. When these frames reach the destination DTE device, the address field (with the FECN bit set) indicates that these frames experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored.
- **Backward explicit congestion notification (BECN):** The BECN bit is in the address field of the Frame Relay frame header. DCE devices set the value of the BECN bit to one in frames that travel in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device can then relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored.

---

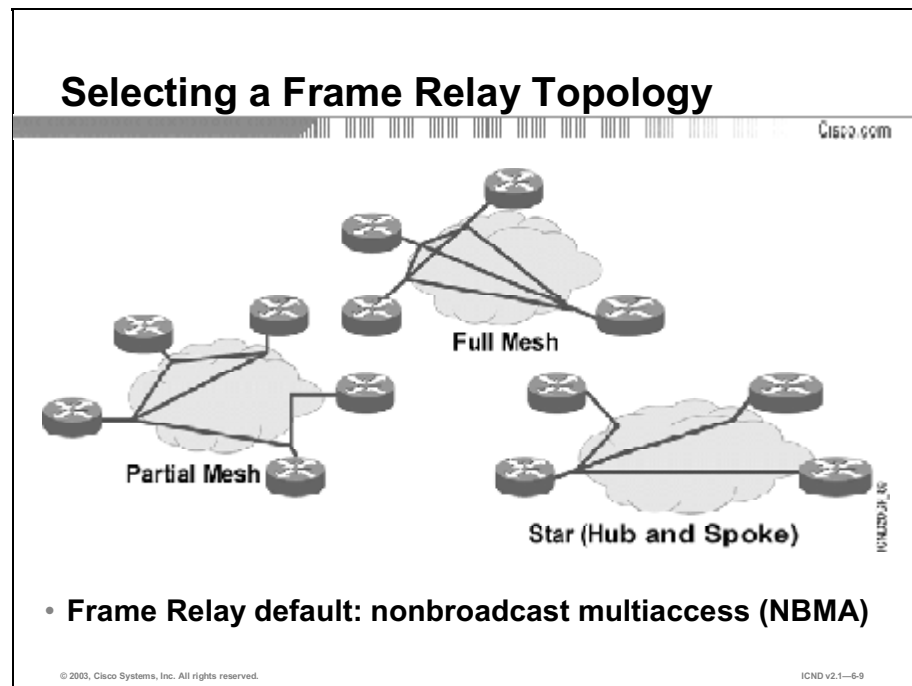
**Note** This topic introduces generic Frame Relay terms. They may be the same or slightly different from the terms your Frame Relay service provider uses. Your Frame Relay equipment may offer flow control and traffic-shaping features that are not covered in this course. For more information regarding Frame Relay flow control and traffic shaping, refer to the *Building Cisco Remote Access Networks (BCRAN)* course.

---



# Frame Relay Topologies

Frame Relay allows you to interconnect your remote sites in a variety of topologies including star, full mesh, and partial mesh. This topic describes the three Frame Relay topologies.



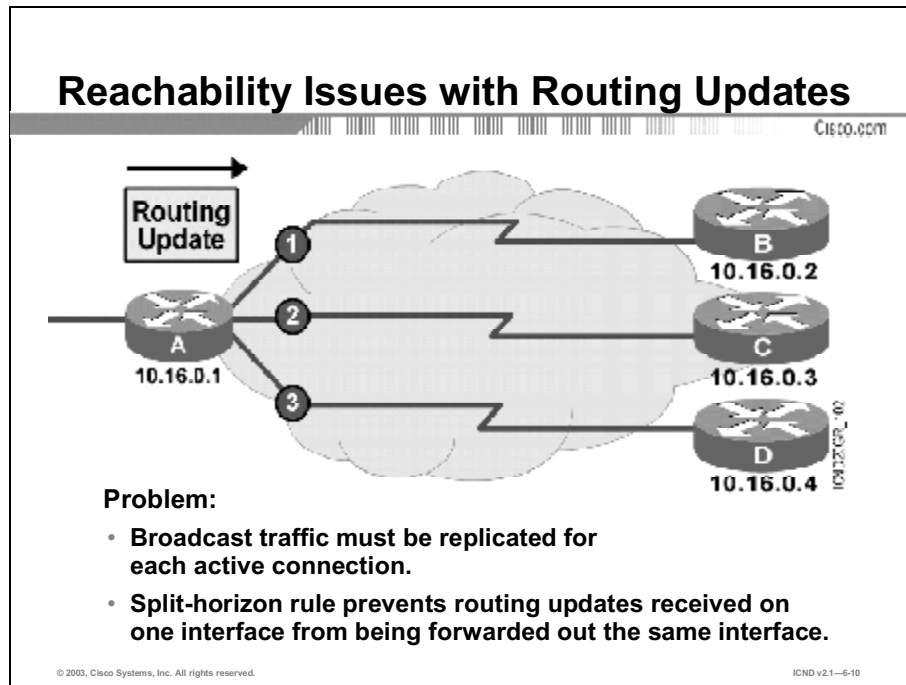
Frame Relay supports the following topologies:

- **Star topology:** A *star topology*, also known as a hub and spoke configuration, is the most popular Frame Relay network topology. In this topology, remote sites are connected to a central site that generally provides a service or application. This is the least expensive topology because it requires the least number of PVCs. In this scenario, the central router provides a multipoint connection because it is typically using a single interface to interconnect multiple PVCs.
- **Full mesh topology:** In a *full mesh topology*, all routers have VCs to all other destinations. This method, although costly, provides direct connections from each site to all other sites and allows for redundancy. When one link goes down, a router can reroute traffic through another site. As the number of nodes in this topology increases, a full mesh topology can become very expensive. Use the  $n(n-1)/2$  formula to calculate the total number of links that are required to implement a full mesh topology, where  $n$  is the number of nodes. For example, to fully mesh a network of 10 nodes,  $10(10-1)/2$  or 45 links are required.
- **Partial mesh topology:** In a *partial mesh topology*, not all sites have direct access to all other sites. Depending on the traffic patterns in your network, you may want to have additional PVCs connect to remote sites that have large data traffic requirements.

In any Frame Relay topology, when a single interface must be used to interconnect multiple sites, you may have reachability issues because of the nonbroadcast multiaccess (NBMA) nature of Frame Relay. With Frame Relay running multiple PVCs over a single interface, the primary issue is with split horizon caused by routing protocols.

# Resolving Reachability Issues in Frame Relay

By default, a Frame Relay network provides an NBMA connectivity between remote sites. An NBMA environment is treated like other broadcast media environments, such as Ethernet, where all the routers are on the same subnet. However, to reduce cost, NBMA clouds are usually built in a hub-and-spoke topology. With a hub-and-spoke topology, the physical topology does not provide the multiaccess capabilities that Ethernet does, so each router may not have separate PVCs to reach the other remote routers on the same subnet. This topic describes the problem of NBMA and offers solutions to the problem.



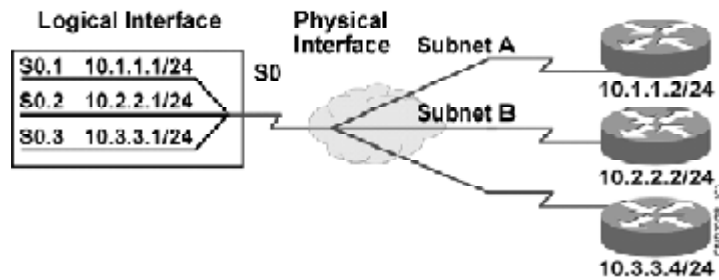
Two problems that the Frame Relay NBMA topology may cause include reachability issues regarding routing updates and the need to replicate broadcasts onto each PVC when a physical interface contains more than one PVC.

First, examine the routing update reachability issue. Split-horizon updates reduce routing loops by not allowing a routing update received on one interface to be forwarded out the same interface. As a result, using a hub-and-spoke Frame Relay topology, if a remote router (a spoke router) sends an update to the headquarter router (the hub router) that is connecting multiple PVCs over a single physical interface, and the headquarter router receives the broadcast on its physical interface, the headquarter router cannot forward that routing update through the same interface to other remote (spoke) routers. Split horizon is not a problem if there is only a single PVC on a physical interface because this would be more of a point-to-point connection type.

Now, examine the broadcast replication issue. With routers that support multipoint connections over a single interface, terminating many PVCs, the router must replicate broadcast packets (like routing update broadcasts) on each PVC to the remote routers. These replicated broadcast packets consume bandwidth and cause significant latency variations in user traffic.

## Resolving Reachability Issues

Cisco.com



- Split horizon can cause problems in NBMA environments.
- Subinterfaces can resolve split-horizon issues.
- Solution: A single physical interface simulates multiple logical interfaces.

© 2003, Cisco Systems, Inc. All rights reserved.

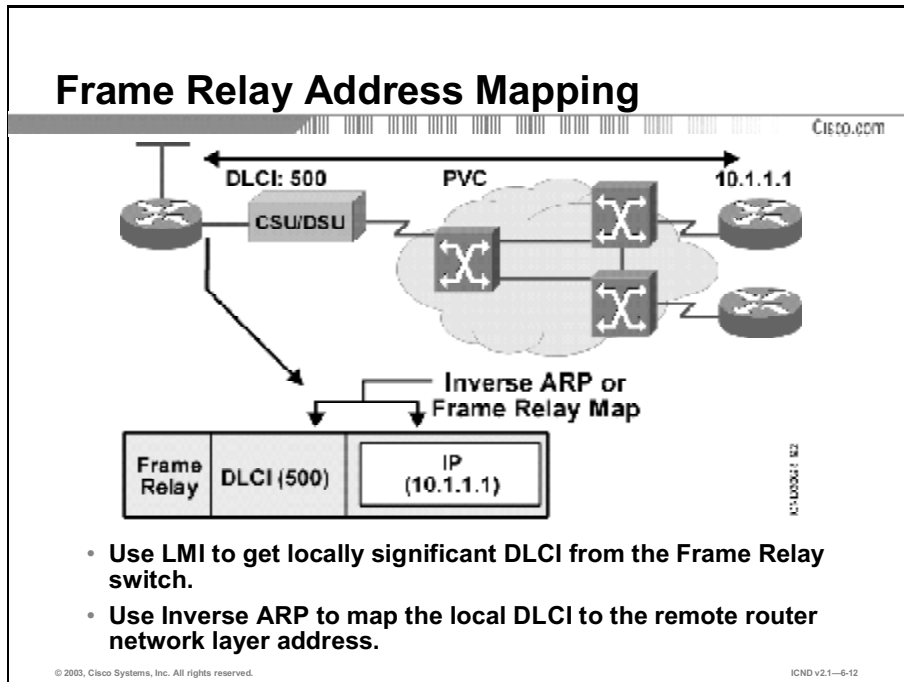
ICND v2.1—6-11

The simplest answer to resolving the reachability issues brought on by split horizon may be to turn off split horizon. Two problems exist with this solution. First, not all network-layer protocols allow you to disable split horizon. (However, most, such as IP, do allow this.) Second, disabling split horizon increases the chances of routing loops in your network.

One way to solve the split-horizon problem is to use a fully-meshed topology; however, this will increase the cost. Another way is to use *subinterfaces*. To enable the forwarding of broadcast routing updates in a hub-and-spoke Frame Relay topology, you can configure the hub router with logically-assigned interfaces called subinterfaces. Subinterfaces are logical subdivisions of a physical interface. In split-horizon routing environments, routing updates received on one subinterface can be sent out another subinterface. In subinterface configuration, each VC can be configured as a point-to-point connection, which allows each subinterface to act similarly to a leased line. Using a Frame Relay point-to-point subinterface, each pair of the point-to-point routers is on its own subnet.

# Frame Relay Address Mapping

A Frame Relay connection requires that, on a VC, the local DLCI is mapped to a destination network layer address, such as an IP address. This topic describes how to map Frame Relay addresses dynamically on Cisco routers.



Routers can automatically discover their local DLCI from the local Frame Relay switch using the Local Management Interface (LMI) protocol.

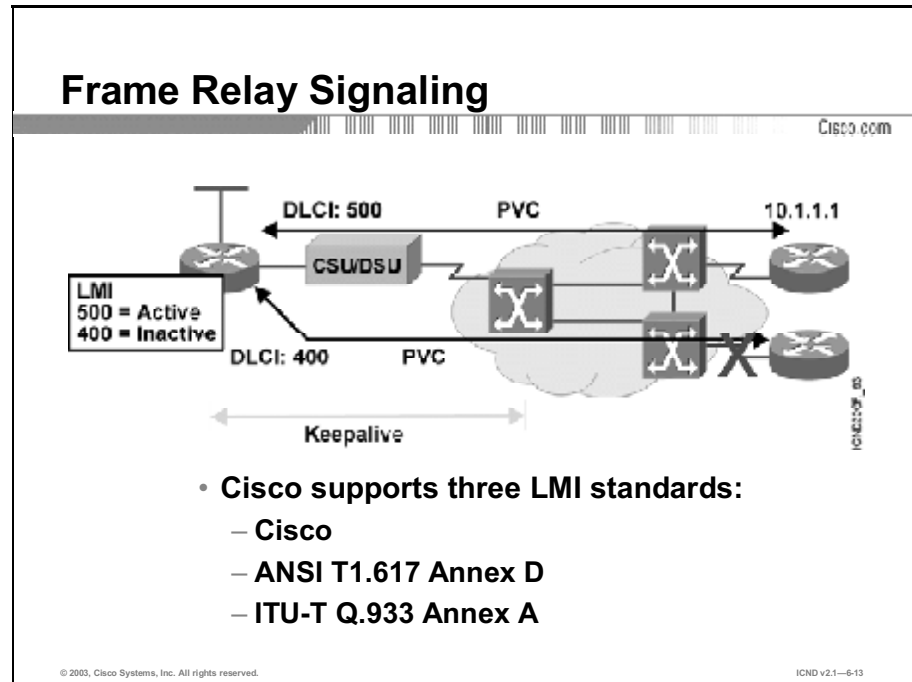
On Cisco routers, the local DLCI can be automatically mapped to the remote router network layer addresses dynamically with Inverse ARP, which associates a given DLCI to the next-hop protocol address for a specific connection. Inverse ARP is described in RFC 1293.

As shown in the figure, using Inverse ARP, the router on the left can automatically discover the remote router IP address and then map it to the local DLCI. In this case, the local DLCI of 500 is mapped to the 10.1.1.1 IP address. Therefore, when the router needs to send data to 10.1.1.1, it uses DLCI 500.

Instead of using Inverse ARP to automatically map the local DLCIs to the remote router network layer addresses, you can manually configure a static Frame Relay map in the map table.

# Frame Relay Signaling

LMI is a signaling standard between the router and the Frame Relay switch. It is responsible for managing the connection and maintaining the status between the devices. This topic describes the LMI signaling standard.



Although the LMI is configurable, beginning in Cisco IOS Release 11.2, the Cisco router tries to autosense which LMI type the Frame Relay switch is using by sending one or more full LMI status requests to the Frame Relay switch. The Frame Relay switch responds with one or more LMI types, and the router configures itself with the last LMI type received. Three types of LMIs are supported, as follows:

- **Cisco:** LMI type defined jointly by Cisco, StrataCom, Northern Telecom, and Digital Equipment Corporation
- **ANSI:** Annex D, defined by the ANSI standard T1.617
- **Q.933A:** ITU-T Q.933 Annex A

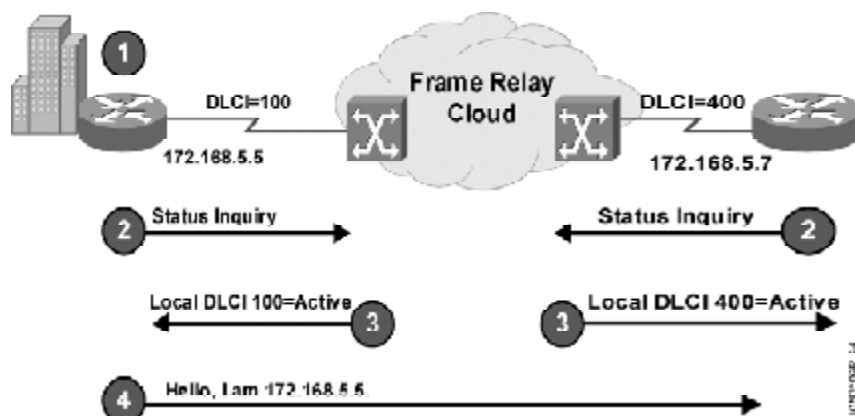
An administrator setting up a connection to a Frame Relay network may choose the appropriate LMI from the three supported types to ensure proper Frame Relay operation.

When the router receives LMI information, it updates its VC status to one of the following three states:

- **Active state:** Indicates that the VC connection is active and that routers can exchange data over the Frame Relay network
- **Inactive state:** Indicates that the local connection to the Frame Relay switch is working, but the remote router connection to the remote Frame Relay switch is *not* working
- **Deleted state:** Indicates that no LMI is being received from the Frame Relay switch, or there is no service between the router and local Frame Relay switch

## Frame Relay Inverse ARP and LMI Signaling

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

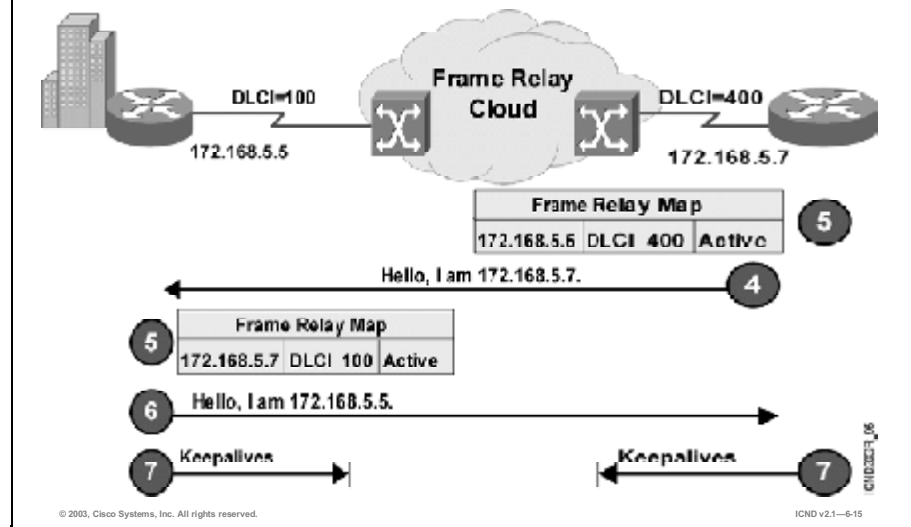
ICND v2.1-6-14

A summary of how Inverse ARP and LMI signaling works with a Frame Relay connection follows:

1. Each router, through a channel service unit/data service unit (CSU/DSU), connects to the Frame Relay switch.
2. When Frame Relay is configured on an interface, the router sends a LMI status inquiry message to the Frame Relay switch. The message notifies the switch of the router status, and asks the switch for the connection status of the router VCs.
3. When the Frame Relay switch receives the request, it responds with an LMI status message that includes the local DLCIs of the PVCs to the remote routers to which the local router can send data.
4. For each active DLCI, each router sends an Inverse ARP packet introducing itself.

## Stages of Inverse ARP and LMI Operation

Cisco.com



- When a router receives an Inverse ARP message, it creates a map entry in its Frame Relay map table that includes the *local* DLCI and the remote router network layer address. Note that the router DLCI is the local DLCI, not the DLCI that the remote router is using. Three possible connection states appear in the Frame Relay map table: active, inactive, and deleted, as previously described.

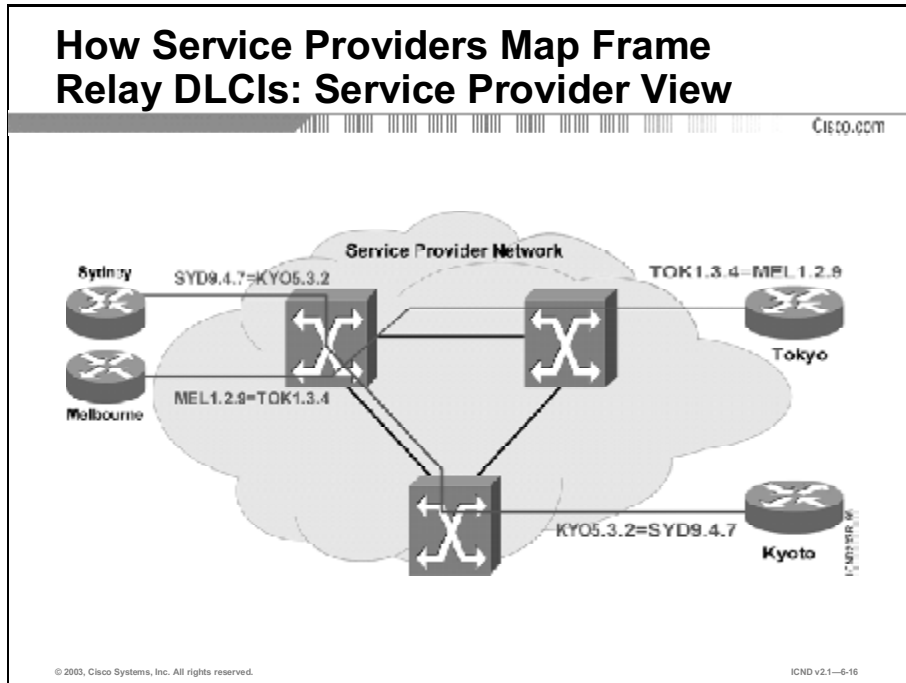
**Note** If Inverse ARP is not working or the remote router does not support Inverse ARP, you must manually configure static Frame Relay maps (mapping the local DLCIs to the remote network layer addresses).

- Every 60 seconds, routers send Inverse ARP messages on all active DLCIs.
- Every 10 seconds, the router exchanges LMI information with the switch (keepalives).

The router will change the status of each DLCI (active, inactive, or deleted), based on the LMI response from the Frame Relay switch.

# How Service Providers Map Frame Relay Data-Link Connection Identifiers

Service providers map Frame Relay DLCIs so that DLCIs with local significance appear at each end of a Frame Relay connection. This topic provides examples showing how service providers map DLCIs.



Within the service provider network, an address maps a local switch.slot.port relationship to a corresponding relationship on a remote switch. The switch contains a table that maps the slot.port to the DLCI at the remote end. When a frame comes into the network, the switch performs the following actions:

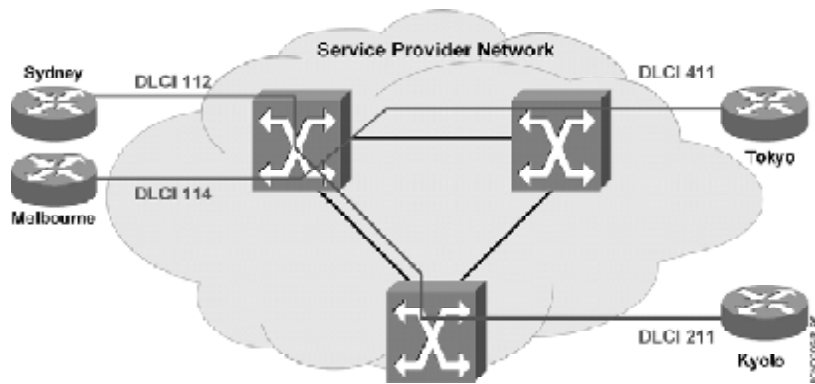
1. The switch checks the inbound DLCI number.
2. The switch looks up the corresponding DLCI number for the remote end.
3. The switch forwards the frame to the appropriate switch.slot.port, including the two DLCI values in the Frame Relay header.

When the frame comes out at the other end, it is already addressed to the DLCI to which it is assigned upon ingress to the network. This permits multiple DLCIs on a single port of a switch.



## How Service Providers Map Frame Relay DLCIs: Enterprise View

Cisco.com



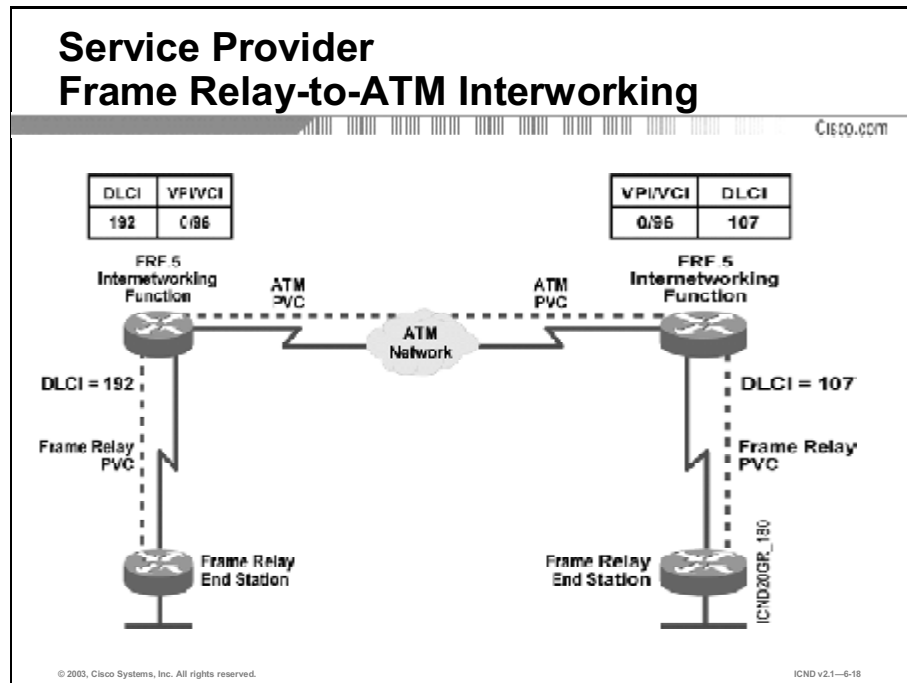
© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-17

The figure reflects a DLCI number plan that inverts the DLCI number at one end to obtain the corresponding DLCI number for the remote end; for example, 112 becomes 211. The enterprise knows that to reach their Melbourne site from the Tokyo site, they use DLCI 411. Similarly, the Melbourne site uses DLCI 114 to reach Tokyo.

# Service Provider Frame Relay-to-ATM Interworking

The ability of ATM to operate at very high speeds and carry a wide range of traffic types has given it an important role as a backbone technology. Today, ATM networks support many Frame Relay services. This topic describes the operation of Frame Relay-to-ATM interworking.

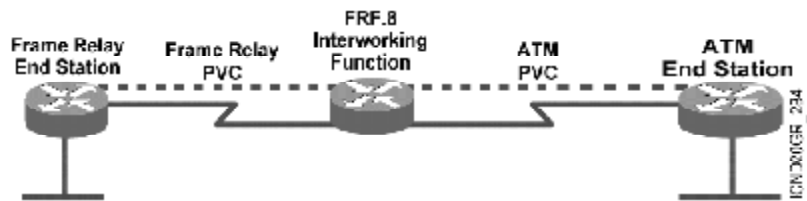


Frame Relay-to-ATM Interworking provides a means to seamlessly integrate Frame Relay and ATM networks. The ATM Forum and Frame Relay Forum have endorsed several implementation agreements that make combining Frame Relay and ATM networks possible. The two implementation agreements that were developed specifically for current Frame Relay users are Network Interworking (FRF.5) and Service Interworking (FRF.8). Both solutions protect current investments in Frame Relay while providing a migration path to ATM.

FRF.5 provides network interworking functionality that allows Frame Relay end users to communicate over an intermediate ATM network that supports FRF.5. Multiprotocol encapsulation and other higher-layer procedures are transported transparently over the ATM network.

## FRF.8 Service Interworking

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-19

FRF.8 provides service interworking functionality that allows a Frame Relay end user to communicate with an ATM end user. A protocol converter translates traffic to provide communication between dissimilar Frame Relay and ATM equipment.

When you configure Frame Relay-to-ATM interworking, the working interface you are configuring is Frame Relay, not ATM.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **Frame Relay is an ITU-T and ANSI standard that defines the process for sending data over a public data network.**
- **The core aspects of Frame Relay function at the lower two layers of the OSI reference model.**
- **Knowing the terms that are used frequently when discussing Frame Relay is important to understanding the operation and configuration of Frame Relay services.**
- **Frame Relay allows you to interconnect your remote sites in a variety of topologies including star, full mesh, and partial mesh.**
- **A Frame Relay NBMA topology may cause routing update reachability issues, which are solved by using subinterfaces.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-20

## Summary (Cont.)

Cisco.com

- **A Frame Relay connection requires that, on a VC, the local DLCI be mapped to a destination network layer address such as an IP address.**
- **LMI is a signaling standard between the router and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices.**
- **Service providers map Frame Relay DLCIs so that DLCIs with local significance appear at each end of a Frame Relay connection.**
- **FRF.5 provides network interworking functionality that allows Frame Relay end users to communicate over an intermediate ATM network that supports FRF.5. FRF.8 provides service interworking functionality that allows a Frame Relay end user to communicate with an ATM end user.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-21

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which three statements accurately describe Frame Relay? (Choose three.)
- A) Frame Relay uses time-division multiplexing.
  - B) Frame Relay is a connection-oriented service.
  - C) Frame Relay provides a mechanism for error detection and correction.
  - D) A connection identifier defines the link between each pair of DTE devices.
  - E) Frame Relay establishes virtual (or logical) circuits over a single physical medium.
  - F) Frame Relay defines how data is transmitted through the service provider network.
- Q2) Frame Relay provides a means for statistically multiplexing many logical data conversations (referred to as \_\_\_\_\_) over a single physical transmission link by assigning connection identifiers to each pair of DTE devices.
- A) table mapping
  - B) virtual circuits
  - C) switched circuits
  - D) data-link connection identifiers (DLCIs)
- Q3) At which layers of the OSI reference model are the core aspects of Frame Relay implemented?
- A) 1 and 2
  - B) 2 and 3
  - C) 3 and 4
  - D) 6 and 7
- Q4) Which five serial connections does a Cisco router support for a Frame Relay connection? (Choose five.)
- A) V.24
  - B) V.35
  - C) V.90
  - D) X.21
  - E) EIA/TIA-232
  - F) EIA/TIA-449
  - G) EIA/TIA-530

- Q5) Which three statements about Frame Relay are true? (Choose three.)
- A) LMI manages the end-to-end connection in a Frame Relay network.
  - B) LMI manages the connection between the router (DTE) and the Frame Relay switch (DCE).
  - C) The DLCI defines the logical circuit between the router (DTE) and the Frame Relay switch (DCE).
  - D) The DLCI defines the logical circuit between the two endpoint routers (DTEs) in a Frame Relay network.
  - E) A PVC is the logical connection created to ensure bidirectional communication between two Frame Relay network DTE devices.
  - F) A PVC is the physical connection created to ensure bidirectional communication between two Frame Relay network DTE devices.
- Q6) Match each Frame Relay operation component to its definition.
- |          |                   |
|----------|-------------------|
| _____ 1. | local access rate |
| _____ 2. | PVC               |
| _____ 3. | LMI               |
| _____ 4. | DLCI              |
- A) identifies the local circuit between the router and the Frame Relay switch
  - B) rate at which data travels into or out of the network, regardless of other settings
  - C) responsible for managing the connection and maintaining the status between the router and the local Frame Relay switch
  - D) saves bandwidth associated with circuit establishment and teardown in situations where certain VCs exist all the time
- Q7) Which Frame Relay topology is the least expensive because it requires the least number of PVCs?
- A) full mesh topology
  - B) partial mesh topology
  - C) star topology (hub-and-spoke)
  - D) combination of star and partial mesh topology
- Q8) In which Frame Relay topology do all routers have VCs to all other routers?
- A) star topology
  - B) full mesh topology
  - C) partial mesh topology
  - D) combination of star and partial mesh topology

- Q9) Split horizon in a NBMA environment does not allow \_\_\_\_\_.  
A) the switch to send the DLCI to the router  
B) the router to send Inverse ARP messages  
C) the router to exchange LMI messages with the switch  
D) routing updates to be sent on the same interface they were received
- Q10) What is the primary purpose of using subinterfaces for Frame Relay?  
A) to conserve valuable IP addresses  
B) to overcome the split-horizon issues  
C) to allow more than one Frame Relay PVC on the router  
D) to allow the use of more than one physical interface for Frame Relay
- Q11) Which two methods can you use to map a network layer address to a Frame Relay DLCI? (Choose two.)  
A) ARP  
B) RARP  
C) DHCP  
D) Inverse ARP  
E) static map commands
- Q12) What does Inverse ARP mapping in a Frame Relay network map?  
A) the local DLCI to the local network layer address  
B) the local DLCI to the remote network layer address  
C) the remote DLCI to the local network layer address  
D) the remote DLCI to the remote network layer address
- Q13) The inactive state for a VC based on the LMI exchange with the Frame Relay switch indicates that \_\_\_\_\_.  
A) there is no LMI being received from the switch  
B) the connection is active and the routers can exchange data  
C) the connection is active, but there is currently no data being exchanged  
D) the local connection to the switch is working, but the remote router connection to the remote switch is not working



- Q14) When a Cisco router sends an LMI status inquiry message to the Frame Relay switch, what does the switch do?
- A) does nothing if the connection is active
  - B) sends an Inverse ARP message back to the router
  - C) sends a status message back to the router that includes the remote DLCI number that the router is connected to
  - D) sends a status message back to the router that includes the local DLCI number of the PVCs to connect to the remote routers
- Q15) On a service provider network that supports Frame Relay, what is the first action that the Frame Relay switch performs when a frame comes into the network?
- A) The switch checks the inbound DLCI number.
  - B) The switch forwards the frame to the appropriate switch.slot.port.
  - C) The switch looks up the corresponding DLCI number for the remote end.
  - D) The switch wraps the two DLCI values in the header of the Frame Relay frame.
- Q16) Service providers map Frame Relay DLCIs so that DLCIs with \_\_\_\_\_ appear at each end of a Frame Relay connection.
- A) large headers
  - B) local significance
  - C) remote significance
  - D) long destination addresses
- Q17) Which two Implementation Agreements have the ATM Forum and the Frame Relay Forum endorsed that make combining Frame Relay and ATM networks possible?
- A) FRF.8 and FRF.5
  - B) FRF.8 and FRF.11
  - C) FRF.8 and FRF.12
  - D) FRF.11 and FRF.5
  - E) FRF.11 and FRF.12

## Quiz Answer Key

- Q1) B, D, E  
**Relates to:** Introducing Frame Relay
- Q2) B  
**Relates to:** Introducing Frame Relay
- Q3) A  
**Relates to:** Frame Relay Stack Layered Support
- Q4) B, D, E, F, G  
**Relates to:** Frame Relay Stack Layered Support
- Q5) B, C, E  
**Relates to:** Frame Relay Terminology
- Q6) 1-B, 2-D, 3-C, 4-A  
**Relates to:** Frame Relay Terminology
- Q7) C  
**Relates to:** Frame Relay Topologies
- Q8) B  
**Relates to:** Frame Relay Topologies
- Q9) D  
**Relates to:** Resolving Reachability Issues in Frame Relay
- Q10) B  
**Relates to:** Resolving Reachability Issues in Frame Relay
- Q11) D, E  
**Relates to:** Frame Relay Address Mapping
- Q12) B  
**Relates to:** Frame Relay Address Mapping
- Q13) D  
**Relates to:** Frame Relay Signaling
- Q14) D  
**Relates to:** Frame Relay Signaling
- Q15) A  
**Relates to:** How Service Providers Map Frame Relay Data-Link Connection Identifiers
- Q16) B  
**Relates to:** How Service Providers Map Frame Relay Data-Link Connection Identifiers
- Q17) A  
**Relates to:** Service Provider Frame Relay-to-ATM Interworking

# Configuring Frame Relay

---

## Overview

You can create Frame Relay connections by connecting routers and access servers directly to the Frame Relay switch, or by connecting routers and access servers directly to a channel service unit/data service unit (CSU/DSU), which then connects to a remote Frame Relay switch. After the hardware is connected, you are ready to configure the Frame Relay service on the router or access server. This lesson explains how to configure a Frame Relay service on a router or access server.

## Relevance

Frame Relay is a Layer 2 WAN technology that is used in many networks throughout the world for data and voice applications. You need to know how to configure Frame Relay as a major WAN service on the internetwork.

## Objectives

Upon completing this lesson, you will be able to:

- Use Cisco IOS commands to configure Frame Relay permanent virtual circuits, given a functioning router
- Use **show** commands to identify anomalies with the Frame Relay permanent virtual circuits, given a functioning router and an operational Frame Relay network
- Use **debug** commands to identify events and anomalies with the Frame Relay permanent virtual circuits, given a functioning router and an operational Frame Relay network

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

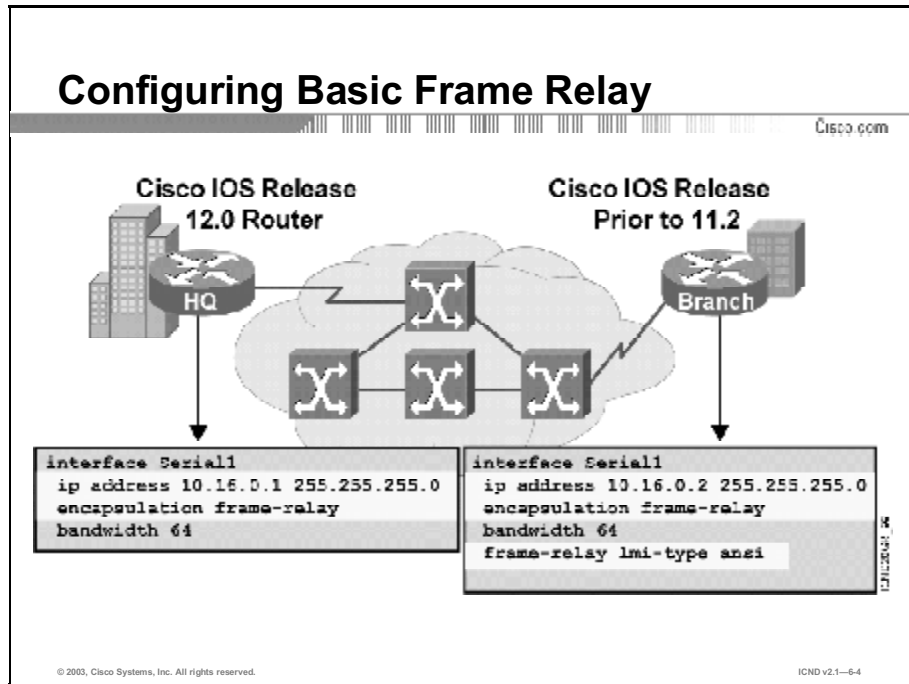
## Outline

This lesson includes these topics:

- Overview
- Configuring a Basic Frame Relay Network
- Configuring a Static Frame Relay Map
- Configuring Frame Relay Subinterfaces
- Verifying Basic Frame Relay Operations
- Troubleshooting Basic Frame Relay Operations
- Summary
- Quiz

# Configuring a Basic Frame Relay Network

A basic Frame Relay configuration assumes that you want to configure Frame Relay on one or more physical interfaces, and that Local Management Interface (LMI) and Inverse Address Resolution Protocol (Inverse ARP) are supported by the router(s). This topic explains how to configure a basic Frame Relay permanent virtual circuit (PVC).



Use the following steps to configure basic Frame Relay:

| Step | Action                                                                                                                                                                                                                                    | Notes                                                                                                                                                                                                                                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Select the interface needed for Frame Relay using the interface configuration mode.<br><br>Router(config)# <b>interface serial1</b>                                                                                                       | After the interface configuration is entered, the CLI <sup>1</sup> prompt will change from (config)# to (config-if)#.                                                                                                                                                                                                                    |
| 2.   | Configure a network layer address; for example, an IP address.<br><br>Router(config-if)# <b>ip address 10.16.0.1 255.255.255.0</b>                                                                                                        |                                                                                                                                                                                                                                                                                                                                          |
| 3.   | Select the Frame Relay encapsulation type used to encapsulate end-to-end data traffic using the <b>encapsulation frame-relay</b> interface configuration command.<br><br>Router(config-if)# <b>encapsulation frame-relay [cisco ietf]</b> | <b>cisco</b> : Uses Cisco encapsulation. Use this option if connecting to another Cisco router. This is the default.<br><br><b>ietf</b> : Sets the encapsulation method to comply with the IETF <sup>2</sup> standard (RFC 1490). Select this if connecting to a router from another vendor.                                             |
| 4.   | Establish LMI connection using the <b>frame-relay lmi-type</b> interface configuration command.<br><br>Router(config-if)# <b>frame-relay lmi-type {ansi   cisco   q933a}</b>                                                              | This command is needed only if using Cisco IOS Release 11.1 or earlier. With Cisco IOS Release 11.2 or later, the LMI type is autosensed, and no configuration is needed.<br><br><b>cisco</b> is the default.<br><br>The LMI type is set on a per-interface basis and is shown in the output of the <b>show interfaces EXEC</b> command. |
| 5.   | Configure the bandwidth for the link using the <b>bandwidth [kilobits]</b> interface configuration command.<br><br>Router(config-if)# <b>bandwidth 64</b>                                                                                 | This command affects routing operation by protocols such as IGRP <sup>3</sup> , EIGRP <sup>4</sup> , and OSPF <sup>5</sup> , as well as other calculations.                                                                                                                                                                              |
| 6.   | Reenable Inverse ARP if it was disabled on the router using the <b>frame-relay inverse-arp [protocol] [dli]</b> interface configuration command.<br><br>Router(config-if)# <b>frame-relay inverse-arp ip 16</b>                           | <b>protocol</b> : Supported protocols include IP, IPX <sup>6</sup> , AppleTalk, DECnet, VINES <sup>7</sup> , and XNS.<br><br><b>dli</b> : The DLCI <sup>8</sup> on the local interface with which you want to exchange Inverse ARP messages.<br><br>Inverse ARP is on by default, and does not appear in the configuration output.       |

<sup>1</sup>CLI = command-line interface

<sup>2</sup>IETF = Internet Engineering Task Force

<sup>3</sup>IGRP = Interior Gateway Routing Protocol

<sup>4</sup>EIGRP = Enhanced Interior Gateway Routing Protocol

<sup>5</sup>OSPF = Open Shortest Path First

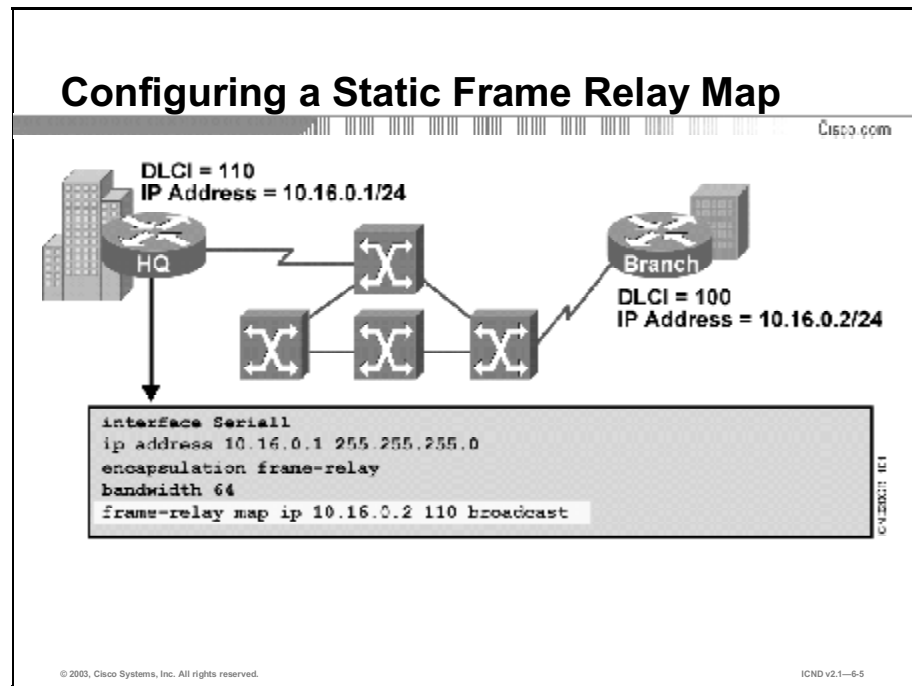
<sup>6</sup>IPX = Internetwork Packet Exchange

<sup>7</sup>VINES = Virtual Integrated Network Service

<sup>8</sup>DLCI = data-link connection identifier

# Configuring a Static Frame Relay Map

When the remote router does not support Inverse ARP, or when you want to control broadcast and multicast traffic over the PVC, you must statically map the local DLCI to the remote router network layer address. These static Frame Relay map entries are referred to as static maps. This topic explains how to configure Frame Relay static maps.



Use the following command to statically map the remote network layer address to the local DLCI:

```
router(config-if)#frame-relay map protocol protocol-address
dlci [broadcast] [ietf | cisco | payload-compress packet-by-
packet]
```

| frame-relay map<br>Command Parameters    | Description                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>protocol</i>                          | Defines the supported protocol, bridging, or logical link control: <b>appletalk</b> , <b>decnet</b> , <b>dlsiw</b> , <b>ip</b> , <b>ipx</b> , <b>llc2</b> , <b>rsrb</b> , <b>vines</b> , and <b>xns</b> . |
| <i>protocol-address</i>                  | Defines the network layer address of the destination router interface.                                                                                                                                    |
| <i>dlci</i>                              | Defines the local DLCI used to connect to the remote protocol address.                                                                                                                                    |
| <b>broadcast</b>                         | (Optional.) Allows broadcasts and multicasts over the VC. This permits the use of dynamic routing protocols over the VC.                                                                                  |
| <b>ietf   cisco</b>                      | Enables <b>ietf</b> or <b>cisco</b> encapsulations.                                                                                                                                                       |
| <b>payload-compress packet-by-packet</b> | (Optional) Enables packet-by-packet payload compression, using the Stacker method. This is a Cisco proprietary compression method.                                                                        |

# Configuring Frame Relay Subinterfaces

You can configure Frame Relay subinterfaces in either point-to-point or multipoint mode. This topic explains how to configure Frame Relay subinterfaces on Cisco routers.

## Configuring Subinterfaces



- **Point-to-point**
  - Subinterfaces act like leased lines.
  - Each point-to-point subinterface requires its own subnet.
  - Point-to-point is applicable to hub and spoke topologies.
- **Multipoint**
  - Subinterfaces act like NBMA networks, so they do not resolve the split-horizon issues.
  - Multipoint can save address space because it uses a single subnet.
  - Multipoint is applicable to partial mesh and full mesh topologies.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—6-6

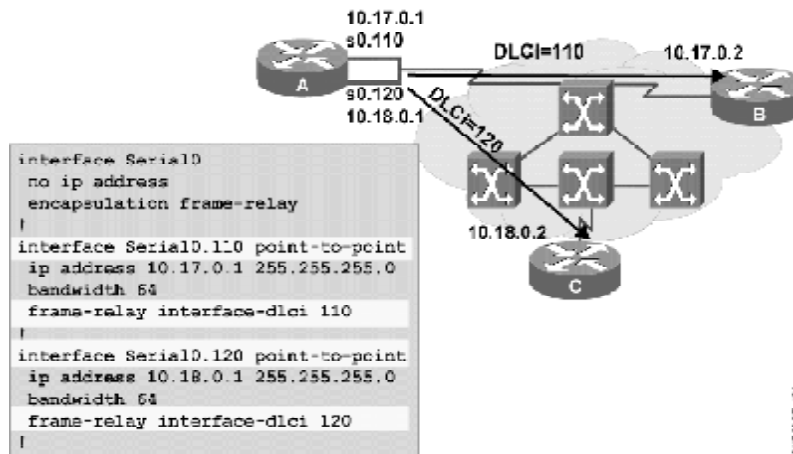
You can configure subinterfaces in one of the following modes:

- **Point-to-point:** A single point-to-point subinterface is used to establish one PVC connection to another physical interface or subinterface on a remote router. In this case, each pair of the point-to-point routers is on its own subnet and each point-to-point subinterface would have a single DLCI. In a point-to-point environment, because each subinterface is acting like a point-to-point interface, routing update traffic is not subject to the split-horizon rule.
- **Multipoint:** A single multipoint subinterface is used to establish multiple PVC connections to multiple physical interfaces or subinterfaces on remote routers. In this case, all the participating interfaces would be in the same subnet. In this environment, because the subinterface is acting like a regular nonbroadcast multi-access (NBMA) Frame Relay interface, routing update traffic is subject to the split-horizon rule.



# Configuring Point-to-Point Subinterfaces

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-7

In the figure, router A has two point-to-point subinterfaces. The s0.110 subinterface connects to router B and the s0.120 subinterface connects to router C. Each subinterface is on a different subnet.

To configure subinterfaces on a physical interface, complete the following:

1. Select the interface that you want to create subinterfaces on and enter interface configuration mode.
2. It is recommended that you remove any network layer address assigned to the physical interface and assign the network layer address to the subinterface.
3. Configure Frame Relay encapsulation.
4. Select the subinterface you want to configure:

```

router(config-if)#interface serial number.subinterface-number
{multipoint | point-to-point}

```

| interface serial<br>Command Parameters | Description                                                                                                                                                                      |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>.subinterface-number</i>            | Subinterface number in the range 1 to 4294967293. The interface number that precedes the period (.) must match the physical interface number to which this subinterface belongs. |
| <b>multipoint</b>                      | Select this if you want all routers in the same subnet.                                                                                                                          |
| <b>point-to-point</b>                  | Select this if you want each pair of point-to-point routers to have its own subnet.                                                                                              |

You are required to select the **multipoint** or **point-to-point** parameter; there is no default.

5. If you configured the subinterface as point-to-point, you must configure the local DLCI for the subinterface to distinguish it from the physical interface. It is also required for multipoint subinterfaces for which Inverse ARP is enabled. It is not required for multipoint subinterfaces configured with static route maps. The command to configure the local DLCI on the subinterface follows:

```
router(config-subif)#frame-relay interface-dlci dlci-number
```

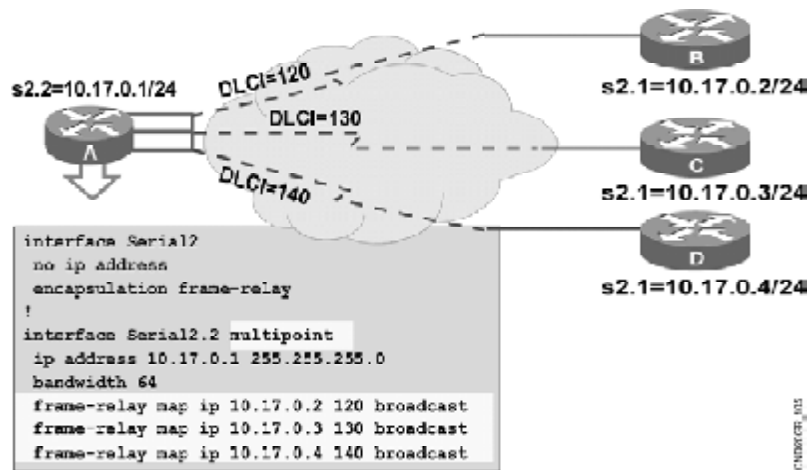
| <b>frame-relay interface-dlci</b><br><b>Command Parameter</b> | <b>Description</b>                                                                                                                                                                |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dlci-number</i>                                            | Defines the local DLCI number being linked to the subinterface. This is the only way to link an LMI-derived DLCI to a subinterface because LMI does not know about subinterfaces. |

Do not use this command on physical interfaces.

|             |                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | If you defined a subinterface for point-to-point communication, you cannot reassign the same subinterface number to use for multipoint communication without first rebooting the router. Instead, you can avoid using that subinterface number by using a different subinterface number. |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Multipoint Subinterfaces Configuration Example

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-8

The configuration output illustrates how to configure multipoint subinterfaces using a static Frame Relay map. With this type of configuration, the subinterface takes on the same Frame Relay characteristics as a physical interface; that is, it is NBMA and is subject to split-horizon operation. The advantage over a point-to-point interface, however, is that you need only a single subnet. In the example, all the routers are on the 10.17.0.0/24 subnet. Router A is configured with a multipoint subinterface with three PVCs. PVC with DLCI 120 is used to connect to router B, PVC with DLCI 130 is used to connect to router C, and PVC with DLCI 140 is used to connect to router D.

Split horizon is disabled by default on Frame Relay multipoint main interfaces, and enabled by default on Frame Relay multipoint subinterfaces. In the example, which uses a multipoint subinterface, split horizon must be manually disabled at router A to overcome the split-horizon issue at router A.

# Verifying Basic Frame Relay Operations

After you configure Frame Relay, you can verify that the connections are active using the available **show** commands. This topic describes the Frame Relay **show** commands.

## Verifying Frame Relay Operation

Router#show frame-relay traffic

- Displays Frame Relay traffic statistics

Router#clear frame-relay-inarp

- Clears dynamically created Frame Relay maps, created by using Inverse ARP

Router#show interfaces type number

- Displays information about Frame Relay DLCIs and the LMI

Router#show frame-relay lmi [type number]

- Displays LMI statistics

Router#show frame-relay map

- Displays the current Frame Relay map entries

Router#show frame-relay pvc [type number [dlci]]

- Displays PVC statistics

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-9

To monitor Frame Relay connections, use any of the following commands in EXEC mode:

| Command                                                | Description                                                                               |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <code>show frame-relay traffic</code>                  | Displays Frame Relay traffic statistics.                                                  |
| <code>clear frame-relay-inarp</code>                   | Clears dynamically created Frame Relay maps, which are created by the use of Inverse ARP. |
| <code>show interfaces type number</code>               | Displays information about Frame Relay DLCIs and the LMI.                                 |
| <code>show frame-relay lmi [type number]</code>        | Displays LMI statistics.                                                                  |
| <code>show frame-relay map</code>                      | Displays the current Frame Relay map entries.                                             |
| <code>show frame-relay pvc [type number [dlci]]</code> | Displays PVC statistics.                                                                  |

## show interfaces Example

Cisco.com

```
Router#show interfaces s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
LMI enq sent 19, LMI stat recvd 20, LMI upd recvd 0, DTE LMI up
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface broadcasts 5
Last input 00:00:02, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
<Output omitted>
```

- Displays line, protocol, DLCI, and LMI information

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-10

The **show interfaces** command displays information regarding the encapsulation and Layer 1 and Layer 2 status. It also displays information about the LMI type, the LMI DLCI, and the Frame Relay data terminal equipment/data circuit-terminating equipment (DTE/DCE) type. Normally, the router will be the DTE. However, a Cisco router can be configured as the Frame Relay switch; in this case, the type will be DCE.

## show frame-relay lmi Example

Cisco.com

```
Router#show frame-relay lmi

LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 113100 Num Status msgs Rcvd 113100
Num Update Status Rcvd 0 Num Status Timeouts 0
```

- Displays LMI information

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-11

Use the **show frame-relay lmi** command to display LMI traffic statistics. For example, this command shows the number of status messages exchanged between the local router and the local Frame Relay switch.

## show frame-relay pvc Example

Cisco.com

```
Router#show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

 input pkts 28 output pkts 10 in bytes 8398
 out bytes 1198 dropped pkts 0 in FECN pkts 0
 in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
 in DE pkts 0 out DE pkts 0
 out bcast pkts 10 out bcast bytes 1198
 pvc create time 00:03:46, last time pvc status changed 00:03:47
```

- Displays PVC traffic statistics

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-12

Use the **show frame-relay pvc** [*interface interface*] [*dcli*] command to display the status of each configured PVC as well as traffic statistics. This command is also useful for viewing the number of backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) packets that are received by the router. The PVC status can be active, inactive, or deleted.

The **show frame-relay pvc** displays the status of all the PVCs configured on the router. If you request a specific PVC, you will see the status of that PVC only. In the figure, the **show frame-relay pvc 100** command displays the status of PVC 100 only.

## show frame-relay map Example

Cisco.com

```
Router#show frame-relay map
Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
 broadcast,, status defined, active
```

- Displays the route maps, either static or dynamic

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-13

Use the **show frame-relay map** command to display the current map entries and information about the connections.

The following information interprets the **show frame-relay map** output that appears in the figure:

- 100 is the decimal local DLCI number.
- 0x64 is the hex conversion of the DLCI number (0x64 = 100 decimal).
- 0x1840 is the “value as it would appear on the wire” because of the way the DLCI bits are spread out in the address field of the Frame Relay frame.
- 10.140.1.1 is the remote router IP address (a dynamic entry learned via the Inverse ARP process).
- Broadcast/multicast is enabled on the PVC.
- PVC status is active.



## clear frame-relay-inarp Example

Cisco.com

```
Router#show frame-relay map
Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
 broadcast,, status defined, active
Router#clear frame-relay-inarp
Router#show frame map
Router#
```

- **Clears dynamically created Frame Relay maps**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-14

To clear dynamically created Frame Relay maps, which are created using Inverse ARP, use the **clear frame-relay-inarp** privileged EXEC command.

# Troubleshooting Basic Frame Relay Operations

Use the **debug frame-relay lmi** command to verify and troubleshoot a Frame Relay connection. This topic describes the **debug frame-relay lmi** command as well as common Frame Relay network problems and possible solutions.

## Troubleshooting Basic Frame Relay Operations

CISCO.COM

```
Router#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router#
lw2d: Serial0(out): StEng, myseq 140, yourseen 139, DTE up
lw2d: datagramstart = 0xE008EC, datagramsize = 13
lw2d: FR encap = 0xFCF10309
lw2d: 00 75 01 01 01 03 02 8C 8B
lw2d:
lw2d: Serial0(in): Status, myseq 140
lw2d: RT IE 1, length 1, type 1
lw2d: KA IE 3, length 2, yourseq 140, myseq 140
lw2d: Serial0(out): StEng, myseq 141, yourseen 140, DTE up
lw2d: datagramstart = 0xE008EC, datagramsize = 13
lw2d: FR encap = 0xFCF10309
lw2d: 00 75 01 01 01 03 02 8D 8C
lw2d:
lw2d: Serial0(in): Status, myseq 142
lw2d: RT IE 1, length 1, type 0
lw2d: KA IE 3, length 2, yourseq 142, myseq 142
lw2d: PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
```

- **Displays LMI debug information**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—6-15

Use the **debug frame-relay lmi** command to determine whether the router and the Frame Relay switch are sending and receiving LMI packets properly.

The “(out)” is an LMI status message sent by the router. The “(in)” is a message received from the Frame Relay switch.

“type 0” is a full LMI status message. “type 1” is an LMI exchange.

The “dlci 100, status 0x2” means that the status of DLCI 100 is active. The possible values of the status field are as follows:

- **0x0:** Added/inactive means that the switch has this DLCI programmed but for some reason (such as, the other end of this PVC is down), it is not usable.
- **0x2:** Added/active means the Frame Relay switch has the DLCI and everything is operational. You can start sending it traffic with this DLCI in the header.
- **0x4:** Deleted means that the Frame Relay switch does not have this DLCI programmed for the router, but that it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the service provider in the Frame Relay cloud.

Connections over a Frame Relay link may fail. The output of the **show interfaces serial** command may show that the interface and line protocol are down, or that the interface is up and the line protocol is down.

The table outlines the problems that might cause this symptom and describes solutions to those problems.

| Possible Problem                                      | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A cabling, hardware, or carrier problem has occurred. | <p>Perform these steps for the local and remote router:</p> <ul style="list-style-type: none"> <li>■ Use the <b>show interfaces serial</b> command to see whether the interface and line protocol are up.</li> <li>■ If the interface and line protocol are down, check the cable to make sure that it is a DTE1 serial cable. Make sure that cables are securely attached.</li> <li>■ If the cable is correct, try moving it to a different port. If that port works, then the first port is defective. Replace either the card or the router.</li> <li>■ If the cable does not work on the second port, try replacing the cable. If it still does not work, there might be a problem with the DCE2. Contact your carrier about the problem.</li> </ul> |
| An LMI-type mismatch has occurred.                    | <ul style="list-style-type: none"> <li>■ Use the <b>show interfaces serial</b> command to check the state of the interface.</li> <li>■ If the output shows that the interface is up but the line protocol is down, use the <b>show frame-relay lmi</b> command to see which LMI type is configured on the Frame Relay interface.</li> <li>■ Make sure that the LMI type is the same for all devices in the path from source to destination. Use the <b>frame-relay lmi-type {ansi   cisco   q933a}</b> interface configuration command to change the LMI type on the router.</li> </ul>                                                                                                                                                                  |
| Keepalives are not being sent.                        | <ul style="list-style-type: none"> <li>■ Enter the <b>show interfaces</b> command to find out whether keepalives are configured. If you see a line that says "keepalives not set," keepalives are not configured.</li> <li>■ Use the <b>keepalive seconds</b> interface configuration command to configure keepalives. The default value for this command is 10 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                      |
| Encapsulation mismatch has occurred.                  | <ul style="list-style-type: none"> <li>■ When connecting Cisco devices with non-Cisco devices, you must use IETF4 encapsulation on both devices. Check the type on the Cisco device with the <b>show frame-relay map</b> command.</li> <li>■ If the Cisco device is not using IETF encapsulation, use the <b>encapsulation frame-relay ietf</b> command to configure IETF encapsulation on the Cisco Frame Relay interface.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| The DLCI is inactive or has been deleted.             | <ul style="list-style-type: none"> <li>■ Use the <b>show frame-relay pvc</b> command to view the status of the interface PVC.</li> <li>■ If the output shows that the PVC6 is inactive or deleted, there is a problem along the path to the remote router. Check the remote router or contact your carrier to check the status of the PVC.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                    |
| The DLCI is assigned to the wrong subinterface.       | <ul style="list-style-type: none"> <li>■ Use the <b>show frame-relay pvc</b> command to check the assigned DLCIs. Make sure that the correct DLCIs are assigned to the correct subinterface. If the DLCI is incorrect, use the <b>no frame-relay map interface-dlci</b> command to delete the incorrect DLCI number entry under the interface.</li> <li>■ Use the <b>frame-relay map interface-dlci</b> command to define the mapping between an address and the correct DLCI used to connect to the address.</li> </ul>                                                                                                                                                                                                                                 |

Attempts to ping the remote router across a Frame Relay connection may fail. The table outlines the problems that might cause this symptom and describes solutions to those problems.

| Possible Problem                               | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encapsulation mismatch has occurred.           | <ul style="list-style-type: none"> <li>■ When connecting Cisco devices with those from other vendors, you must use IETF encapsulation on both devices. Check the encapsulation type on the Cisco device with the <b>show frame-relay map</b> command.</li> <li>■ If the Cisco device is not using IETF encapsulation, use the <b>encapsulation frame-relay ietf</b> command to configure IETF encapsulation on the Cisco Frame Relay interface.</li> </ul>                                           |
| DLCI is inactive or has been deleted.          | <ul style="list-style-type: none"> <li>■ Use the <b>show frame-relay pvc</b> command to view the status of the interface PVC.</li> <li>■ If the output shows that the PVC is inactive or deleted, there is a problem along the path to the remote router. Check the remote router, or contact your carrier to check the status of the PVC.</li> </ul>                                                                                                                                                |
| DLCI is assigned to the wrong subinterface.    | <ul style="list-style-type: none"> <li>■ Use the <b>show frame-relay pvc</b> command to check the assigned DLCIs. Make sure that the correct DLCIs are assigned to the correct subinterfaces.</li> <li>■ If the DLCIs appear to be correct, shut down the main interface using the <b>shutdown</b> command, and then bring the interface back up using the <b>no shutdown</b> command.</li> </ul>                                                                                                    |
| The <b>frame-relay map</b> command is missing. | <ul style="list-style-type: none"> <li>■ Use the <b>show frame-relay map</b> command to see whether an address map is configured for the DLCI.</li> <li>■ If you do not see an address map for the DLCI, enter the clear frame-relay-inarp privileged EXEC command and then use the <b>show frame-relay map</b> command again to see whether there is now a map to the DLCI.</li> <li>■ If there is no map to the DLCI, add a static address map. Use the <b>frame-relay map</b> command.</li> </ul> |

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary



- **A basic Frame Relay configuration assumes one or more physical interfaces, and LMI and Inverse ARP are running on the remote routers. In this type of environment, the LMI notifies the router about the available DLCIs.**
- **When the remote router does not support Inverse ARP, or when you want to control routed broadcast traffic, you must define the address-to-DLCI table statically.**
- **You can configure Frame Relay subinterfaces in either point-to-point or multipoint mode.**
- **After you configure Frame Relay, you can verify that the connections are active using the available show commands.**
- **Use the debug frame-relay lmi command to verify and troubleshoot a Frame Relay connection.**

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—6-16

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

## Next Steps

After completing this lesson, go to:

- Lab Exercise 6-1: Connecting to Frame Relay Services

# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) The **encapsulation frame-relay** command is configured on a Cisco router interface. What type of encapsulation will be used on the interface?

- A) LMI
- B) IETF
- C) ANSI
- D) Cisco

Q2) Which Cisco IOS command correctly establishes an LMI connection for Cisco IOS Release 11.2 or later?

- A) **frame-relay lmi-type cisco**
- B) **frame-relay inverse-arp ip 16**
- C) **encapsulation frame-relay cisco**
- D) **no configuration needed, use autosense LMI**

Q3) The following statement was configured on the Cisco router:

```
frame-relay map ip 10.16.0.2 110 broadcast ietf
```

Which statement is true?

- A) The remote IP address is 10.16.0.2; the local DLCI is 110; only ietf broadcasts will be forwarded.
- B) The local IP address is 10.16.0.2; the remote DLCI is 110; broadcasts will be forwarded; the encapsulation is ietf.
- C) The local IP address is 10.16.0.2; the local DLCI is 110; broadcasts will be forwarded; the encapsulation is ietf.
- D) The remote IP address is 10.16.0.2; the local DLCI is 110; broadcasts will be forwarded; the encapsulation is ietf.

Q4) Which Cisco IOS command correctly configures a static map of the remote network layer address (10.16.0.2) to the local DLCI (110) but does not allow broadcasts and multicasts over the virtual circuit?

- A) **frame-relay map ip 10.16.0.2 110**
- B) **frame-relay map ip 10.16.0.2 110 broadcast**
- C) **frame-relay map ip 10.16.0.2 110 no broadcast**
- D) **frame-relay map ip 10.16.0.2 110 no broadcast multicast**

- Q5) Which two types of Frame Relay subinterfaces can you configure on a Cisco router? (Choose two.)
- A) multipoint
  - B) point-to-point
  - C) point-to-multipoint
  - D) multipoint-to-point
  - E) multipoint-to-multipoint
- Q6) When configuring subinterfaces on a Cisco router, what should you configure on the physical interface?
- A) IP address only
  - B) DLCI number only
  - C) Frame Relay encapsulation only
  - D) IP address and Frame Relay encapsulation
- Q7) Which Cisco IOS command verifies the encapsulation configured on the serial 0 interface of a Cisco router?
- A) **show s0 interfaces**
  - B) **show interfaces s0**
  - C) **show s0 frame-relay**
  - D) **show s0 frame-relay interfaces**
- Q8) Which Cisco IOS command removes all dynamically created maps?
- A) **Router#clear frame-relay-inarp**
  - B) **Router(config)#clear frame-relay-inarp**
  - C) **Router(config-if)#clear frame-relay map**
  - D) **Router(config-if)#clear frame-relay-inarp**
- Q9) The following line is taken from the output of the **debug frame-relay lmi** command:

```
1w2d: RT IE 1, length 1, type 1
```

What does the **type 1** indicate?

- A) a full LMI status message
- B) an LMI exchange message
- C) message originated at the router
- D) message is sent using DLCI number 1

Q10) The following line is taken from the output of the **debug frame-relay lmi** command:

```
1w2d: PVC IE 0x7, length 0x6, dlci 100, status 0x2, bw 0
```

What does the **dlci 100 status 0x2** indicate?

- A) DLCI 100 is inactive, the status is deleted
- B) DLCI 100 is active, the status is added/active
- C) DLCI 100 is active, the status is added/inactive
- D) DLCI 100 is inactive, the status is added/inactive



## Quiz Answer Key

- Q1) D  
**Relates to:** Configuring a Basic Frame Relay Network
- Q2) D  
**Relates to:** Configuring a Basic Frame Relay Network
- Q3) D  
**Relates to:** Configuring a Static Frame Relay Map
- Q4) A  
**Relates to:** Configuring a Static Frame Relay Map
- Q5) A, B  
**Relates to:** Configuring Frame Relay Subinterfaces
- Q6) C  
**Relates to:** Configuring Frame Relay Subinterfaces
- Q7) B  
**Relates to:** Verifying Basic Frame Relay Operations
- Q8) A  
**Relates to:** Verifying Basic Frame Relay Operations
- Q9) B  
**Relates to:** Troubleshooting Basic Frame Relay Operations
- Q10) B  
**Relates to:** Troubleshooting Basic Frame Relay Operations



# Lesson Assessments

---

## Overview

Use the lesson assessments here to test what you have learned in this module. The correct answers and solutions follow in the Lesson Assessment Answer Key.

## Outline

This topic includes these assessments:

- Lesson Assessment 6-1: Frame Relay Overview
- Lesson Assessment 6-2: Configuring Frame Relay

# Lesson Assessment 6-1: Frame Relay Overview

Complete the quiz to assess what you learned in this lesson.

## Objectives

This quiz tests your knowledge of how to:

- Describe the features and operation of a Frame Relay network
- Define important Frame Relay terms, including local access rate, virtual circuit, permanent virtual circuit, switched virtual circuit, data-link connection identifier, committed information rate, inverse Address Resolution Protocol, Local Management Interface, forward explicit congestion notification, and backward explicit congestion notification

## Instructions

Answer these questions:

- Q1) Frame Relay is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and American National Standards Institute (ANSI) standard that defines the process for sending data over a \_\_\_\_\_.  
A) leased-line service  
B) public data network  
C) circuit-switched network  
D) public telephone network
- Q2) What does Frame Relay define?  
A) error correction  
B) how data is transmitted inside the service provider Frame Relay cloud  
C) interconnection process between a Frame Relay switch and the service provider local routing equipment  
D) interconnection process between the router and the service provider local access Frame Relay switching equipment
- Q3) Working at the \_\_\_\_\_ layer, Frame Relay encapsulates information from the upper layers of the Open System Interconnection (OSI) reference model.  
A) session  
B) physical  
C) network  
D) data-link
- Q4) Which two layers of the OSI model support the core aspects of Frame Relay?  
A) 1 and 2  
B) 2 and 3  
C) 3 and 4  
D) 4 and 5

Q5) Match each Frame Relay operation component to its definition.

- \_\_\_\_\_ 1. local access rate
- \_\_\_\_\_ 2. switched virtual circuit (SVC)
- \_\_\_\_\_ 3. committed information rate (CIR)
- \_\_\_\_\_ 4. Local Management Interface (LMI)
- \_\_\_\_\_ 5. Inverse Address Resolution Protocol (ARP)
- A) maximum average data rate
- B) clock speed of the connection to the Frame Relay cloud
- C) method of dynamically associating a remote network layer address with a local data-link connection identifier (DLCI)
- D) virtual circuit (VC) that is dynamically established on demand and is torn down when transmission is complete
- E) signaling standard between the router device and the Frame Relay switch that is responsible for managing the connection and maintaining status between the devices

Q6) \_\_\_\_\_ is a number that identifies the logical circuit between the router and the local Frame Relay switch.

- A) A data-link connection identifier (DLCI)
- B) A Local Management Interface (LMI) signal
- C) A forward explicit congestion notification (FECN) packet
- D) A backward explicit congestion notification (BECN) packet

Q7) Match each Frame Relay topology to its description.

- \_\_\_\_\_ 1. star
- \_\_\_\_\_ 2. full mesh
- \_\_\_\_\_ 3. partial mesh
- A) All routers have virtual circuits to all other destinations.
- B) Many, but not all routers, have direct access to all other sites.
- C) Remote sites are connected to a central site that generally provides a service or application.

Q8) In any Frame Relay topology, when a single interface must be used to interconnect multiple sites, you may have reachability issues because of the \_\_\_\_\_ nature of Frame Relay.

- A) intermittent
- B) point-to-point
- C) error correcting
- D) nonbroadcast multiaccess (NBMA)

- Q9) A Frame Relay connection requires that, on a VC, the local DLCI be mapped to a destination \_\_\_\_\_ address, such as an IP address.
- A) port
  - B) or source
  - C) network layer
  - D) data-link layer
- Q10) What is an alternative method to using Inverse ARP to map DLCIs to network layer addresses on a Frame Relay network?
- A) ARP
  - B) RARP
  - C) DHCP
  - D) static map commands
- Q11) Which three LMI types does Cisco support? (Choose three.)
- A) DEC
  - B) ANSI
  - C) Cisco
  - D) Q.931
  - E) Q.933A
- Q12) Which VC status state on a Cisco router indicates that the local connection to the Frame Relay switch is working but the remote router connection to the Frame Relay switch is not working?
- A) LMI state
  - B) active state
  - C) deleted state
  - D) inactive state
- Q13) On a service provider network that supports Frame Relay, what is the last action that the Frame Relay switch performs to route a frame?
- A) The switch checks the inbound DLCI number.
  - B) The switch forwards the frame to the appropriate switch.slot.port.
  - C) The switch looks up the corresponding DLCI number for the remote end.
  - D) The switch wraps the two DLCI values in the header of the Frame Relay frame.
- Q14) What type of network technology do service providers typically use in their network core?
- A) IP
  - B) ATM
  - C) Frame Relay
  - D) circuit-switched

- Q15) Which Frame Relay Forum standard defines the Frame Relay-to-ATM Interworking function?
- A) FRF.5
  - B) FRF.8
  - C) FRF.11
  - D) FRF.12
- Q16) When you configure Frame Relay-to-ATM interworking, what interface are you configuring?
- A) IP
  - B) serial
  - C) ATM
  - D) Frame Relay

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment 6-2: Configuring Frame Relay

Complete the quiz to assess what you learned in this lesson.

## Objectives

This quiz tests your knowledge of how to:

- Use Cisco IOS commands to configure Frame Relay permanent virtual circuits, given a functioning router
- Use **show** commands to identify anomalies with the Frame Relay permanent virtual circuits, given a functioning router and an operational Frame Relay network
- Use **debug** commands to identify events and anomalies with the Frame Relay permanent virtual circuits, given a functioning router and an operational Frame Relay network

## Instructions

Answer these questions:

Q1) Which configuration configures a Frame Relay network with the following parameters:

- Interface is Serial 0
  - IP address is 10.12.10.10
  - Subnet mask is 255.255.255.0
  - Set encapsulation for a Cisco router
  - Use IOS Release 12.0 (LMI-type is autosensing)
  - Bandwidth is set for 64 kbps
  - Inverse ARP is already enabled
- A) **Router(config)#interface serial0 (correct)**  
**Router(config-if)#ip address 10.12.10.10 255.255.255.0**  
**Router(config-if)#encapsulation frame-relay cisco**  
**Router(config-if)#bandwidth 64**
- B) **Router(config)#interface serial0**  
**Router(config-if)#ip address 10.12.10.10 255.255.255.0**  
**Router(config-if)#encapsulation frame-relay**  
**Router(config-if)#bandwidth 64000**
- C) **Router(config)#interface serial0**  
**Router(config-if)#ip address 10.12.10.10 255.255.255.0**  
**Router(config-if)#encapsulation frame-relay ietf**  
**Router(config-if)#bandwidth 64**
- D) **Router(config)#interface serial0**  
**Router(config-if)#encapsulation frame-relay cisco**  
**Router(config-if)#bandwidth 64000**



- Q2) In which situation will you configure a static Frame Relay map?
- A) when compression is not set on the interface
  - B) when the remote router does not support Inverse ARP
  - C) when the remote router does not support Frame Relay
  - D) when the network layer address of the destination router interface is not set
- Q3) Which Cisco IOS command correctly configures a static map of the remote IP address (10.16.0.2) to the local data-link connection identifier (DLCI) (110)?
- A) **frame-relay map dlci 110 ip 10.16.0.2**
  - B) **frame-relay inverse-arp ip 10.16.0.2 110**
  - C) **frame-relay arp ip 10.16.0.2 110 broadcast**
  - D) **frame-relay map ip 10.16.0.2 110 broadcast**
- Q4) When trying to resolve reachability issues brought on by split horizon, you should not turn off split horizon. Which two problems are present when you turn off split horizon? (Choose two.)
- A) Routing updates must be replicated for each permanent virtual circuit (PVC).
  - B) You cannot turn off split horizon on an IP network.
  - C) You cannot disable split horizon for point-to-point connections.
  - D) Not all network layer protocols allow you to disable split horizon.
  - E) Disabling split horizon increases the chance of routing loops in your network.
- Q5) To enable the forwarding of broadcast routing updates in a hub-and-spoke Frame Relay topology, you can configure the hub router with logically assigned interfaces called \_\_\_\_\_.
- A) broadcast links
  - B) multipoint connections
  - C) point-to-point subinterfaces
  - D) point-to-multipoint interface
- Q6) Which Cisco IOS command displays the current Frame Relay map entries?
- A) **show frame-relay map**
  - B) **show frame-relay route**
  - C) **show interfaces *interface***
  - D) **show frame-relay pvc *type number dlci***
- Q7) Match each Frame Relay **show** command to its description.
- |          |                                 |
|----------|---------------------------------|
| _____ 1. | <b>show frame-relay lmi</b>     |
| _____ 2. | <b>show frame-relay map</b>     |
| _____ 3. | <b>show frame-relay pvc</b>     |
| _____ 4. | <b>show frame-relay traffic</b> |
- A) displays Local Management Interface (LMI) statistics
  - B) displays PVC statistics
  - C) displays Frame Relay traffic statistics
  - D) displays the current Frame Relay map entries

Q8) The following line is taken from the output of the **debug frame-relay lmi** command:

```
1w2d: PVC IE 0x7, length 0x6, dlci 10, status 0x2, bw 0
```

What does the **dlci 10 status 0x2** indicate?

- A) DLCI 10 is inactive, the status is deleted.
  - B) DLCI 10 is active, the status is added/active.
  - C) DLCI 10 is active, the status is added/inactive.
  - D) DLCI 10 is inactive, the status is added/inactive.
- Q9) If you use the **debug frame-relay lmi** command, what are two causes of a **0x4** status command for a DLCI? (Choose two.)
- A) The DLCI is active and operational.
  - B) The DLCIs could be reversed on the router.
  - C) The DLCI is inactive, maybe the other end of the PVC is down.
  - D) The PVC could have been deleted by the service provider in the Frame Relay cloud.

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment Answer Key

## Lesson Assessment 6-1: Frame Relay Overview

- Q1) B
- Q2) D
- Q3) D
- Q4) A
- Q5) B, D, A, E, C
- Q6) A
- Q7) C, A, B
- Q8) D
- Q9) C
- Q10) D
- Q11) B, C, E
- Q12) D
- Q13) B
- Q14) B
- Q15) A
- Q16) D

## Lesson Assessment 6-2: Configuring Frame Relay

- Q1) A
- Q2) B
- Q3) D
- Q4) D, E
- Q5) C
- Q6) A
- Q7) A, D, B, C
- Q8) B
- Q9) B, D



# Completing ISDN Calls

---

## Overview

ISDN is an all-digital network service. This module deals exclusively with what is known as narrowband ISDN. ISDN has replaced the use of analog modems for many who need fast intermittent access to dial-up networks.

Dial-on-demand routing (DDR) addresses the need for intermittent network connections over circuit-switched WANs. With DDR, all traffic is classified as either interesting or uninteresting. If traffic is interesting, the packet is passed to the interface, and the router then connects to the remote router (if not currently connected). DDR is implemented in two ways: DDR with dialer profiles and legacy DDR. This module describes how to configure DDR between two routers with Basic Rate Interface (BRI) or Primary Rate Interface (PRI).

Upon completing this module, you will be able to:

- Configure ISDN BRI, ISDN PRI, and legacy DDR, given a functioning remote access router and a physical ISDN connection
- Use **show** commands to identify the anomalies in the ISDN BRI, ISDN PRI, and legacy DDR configurations, given a functioning remote access router and a physical ISDN connection
- Use **debug** commands to identify the anomalies in the ISDN BRI, ISDN PRI, and legacy DDR configurations, given a functioning remote access router and a physical ISDN connection

## Outline

The module contains these lessons:

- Configuring ISDN BRI and PRI
- Configuring Dial-on-Demand Routing
- Lesson Assessments



# Configuring ISDN BRI and PRI

---

## Overview

ISDN provides dial-up connectivity to a service provider network similar to standard modem connectivity, but uses digital technology end to end. This allows for a variety of digital transport uses, including video, voice, and data, as well as enabling faster call setup time. This lesson describes ISDN Basic Rate Interface (BRI) and ISDN Primary Rate Interface (PRI).

## Relevance

ISDN configuration is considered to be complex and error-prone. If you use an ISDN interface, this module will show you the basics of how to configure your Cisco device for that purpose.

## Objectives

Upon completing this lesson, you will be able to:

- Configure ISDN BRI and ISDN PRI, given a functioning router and a physical ISDN connection
- Use **show** commands to identify the anomalies in the ISDN BRI and PRI configurations, given a functioning router and a physical ISDN connection
- Use **debug** commands to identify the anomalies in the ISDN BRI and PRI configurations, given a functioning remote access router and a physical ISDN connection

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

# Outline

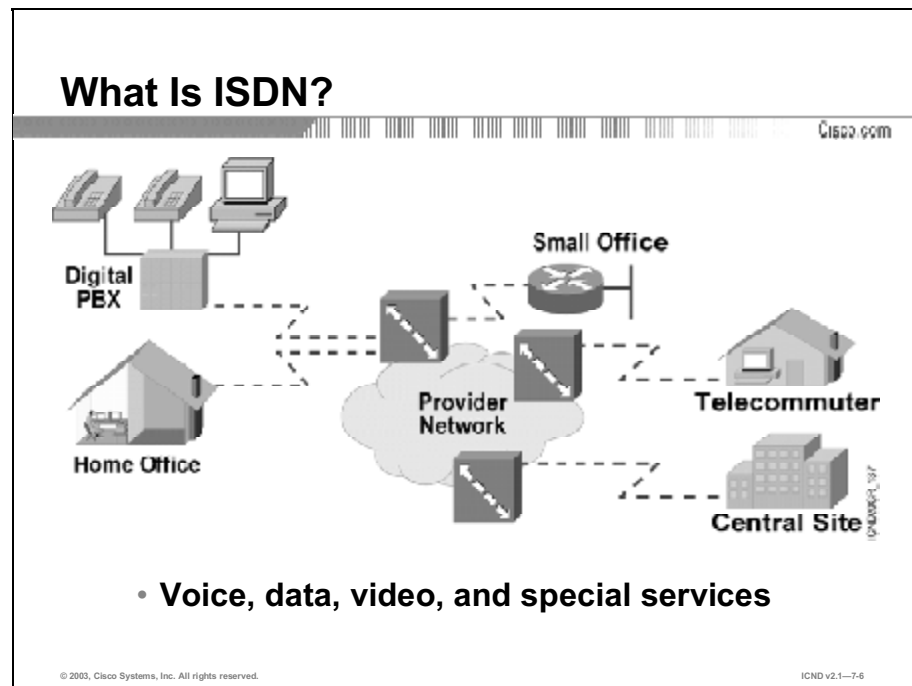
This lesson includes these topics:

- Overview
- Introducing ISDN
- ISDN Standards and Access Methods
- Establishing an ISDN BRI or PRI Call
- ISDN Functions and Reference Points
- Determining the Router ISDN Interface
- ISDN Switch Types
- Configuring ISDN BRI
- Configuring ISDN PRI
- Verifying the ISDN Configuration
- Troubleshooting the ISDN Configuration
- Summary
- Quiz



# Introducing ISDN

ISDN defines a digital architecture that provides integrated voice and data capability using the public switched network. This topic describes the basic capabilities that ISDN offers.



ISDN stands for Integrated Services Digital Network. It refers to a collection of standards that define a digital architecture that provides integrated voice/data capability, utilizing the public switched network. The ISDN standards define the interface specifications. Prior to ISDN, many telephone companies used digital networks within their clouds, but used analog lines for the local access loop between the cloud and the actual customer site. Bringing digital connectivity via ISDN to the local loop has many advantages, including the following:

- The ability to carry a variety of user-traffic feeds. ISDN provides access to all-digital facilities for video, telex, packet-switched data, and enriched telephone network services.
- Much faster call setup than modem connections by using out-of-band (D, or delta, channel) signaling. For example, ISDN calls can often be set up and completed in less than a second.
- Much faster data transfer rate using bearer (B)- channel services at 64 kbps per channel as opposed to common modem rates up to 56 kbps. With multiple B channels, ISDN offers users more bandwidth on WANs (for example, the two B channels of a basic rate interface equal 128 kbps) than they receive with a leased line at 56 kbps in North America or 64 kbps in much of the rest of the world.

In general, ISDN has become the transport of choice in many parts of the world for applications using remote connectivity and access to the Internet. Even with the challenges of digital subscriber lines (DSL) and cable modems, ISDN continues to grow, outpacing these newer and faster technologies with the number of channels installed. Market analysts predict this will be the case at least until 2004.

# ISDN Standards and Access Methods

ISDN specifies two standard access methods, Basic Rate Interface (BRI) and Primary Rate Interface (PRI). This topic describes the ISDN standards and the two access methods.

| ISDN Standards                         |          |                                                                                                             |
|----------------------------------------|----------|-------------------------------------------------------------------------------------------------------------|
| Issue                                  | Protocol | Key Examples                                                                                                |
| Telephone network and ISDN             | E-series | E.163—International telephone numbering plan<br>E.164—International addressing                              |
| ISDN concepts, aspects, and interfaces | I-series | I.100 Series—Concepts, structures, terminology<br>I.400—User-Network Interfaces (UNIs)                      |
| Switching and signaling                | Q-series | Q.921—LAPD (Link Access Procedure on the D channel)<br>Q.931—ISDN network layer between terminal and switch |

• Standards from the ITU-T

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—7-7

Work on standards for ISDN began in the late 1960s. A comprehensive set of ISDN recommendations was published in 1984 and is continuously updated by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), which groups and organizes the ISDN protocols according to the following general topic areas:

- Protocols that begin with “E” recommend telephone network standards for ISDN. For example, the E.164 protocol describes international addressing for ISDN.
- Protocols that begin with “I” deal with concepts, terminology, and general methods. The I.100 series includes general ISDN concepts and the structure of other I-series recommendations; I.200 deals with service aspects of ISDN; I.300 describes network aspects; I.400 describes how the User-Network Interface (UNI) is provided.
- Protocols that begin with “Q” cover how switching and signaling should operate. The term *signaling* in this context means the process of the call set used. Q.921 describes the ISDN *data-link* processes of the Link Access Procedure on the D channel (LAPD), which functions like Layer 2 processes in the Open System Interconnection (OSI) reference model. Q.931 specifies OSI reference model Layer 3 functions.

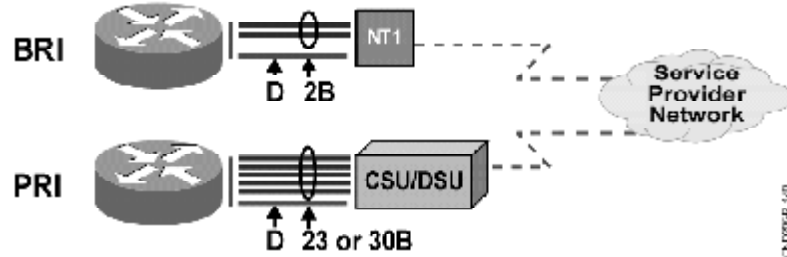
Q.931 recommends a network layer between the terminal endpoint and the local ISDN switch. This protocol does not impose an end-to-end recommendation. The various ISDN providers and switch types can and do use various implementations of Q.931. Other switches were developed before the standards groups finalized this standard.

Because switch types are not standard, when configuring the router, you will need to specify the ISDN switch to which you are connecting. In addition, Cisco Systems routers have **debug** commands to monitor Q.931 and Q.921 processes when an ISDN call is initiated or terminated.

## ISDN Access Options

Cisco.com

| Channel | Capacity   | Mostly Used For                   |
|---------|------------|-----------------------------------|
| B       | 64 kbps    | Circuit-switched data (HDLC, PPP) |
| D       | 16/64 kbps | Signaling information (LAPD)      |



- **BRI and PRI are used globally for ISDN.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-8

ISDN specifies two standard access methods, as follows:

- **BRI:** Two 64-kbps B channels plus one 16-kbps D-channel service. BRI operates with many Cisco routers.

BRI is sometimes written as 2B+D. This interface provides two B channels at 64 kbps and an additional 16-kbps D-signaling channel.

The B channels can be used for digitized speech transmission or for relatively high-speed data transport. Narrowband ISDN is circuit-switching oriented. The B channel is the elemental circuit-switching unit.

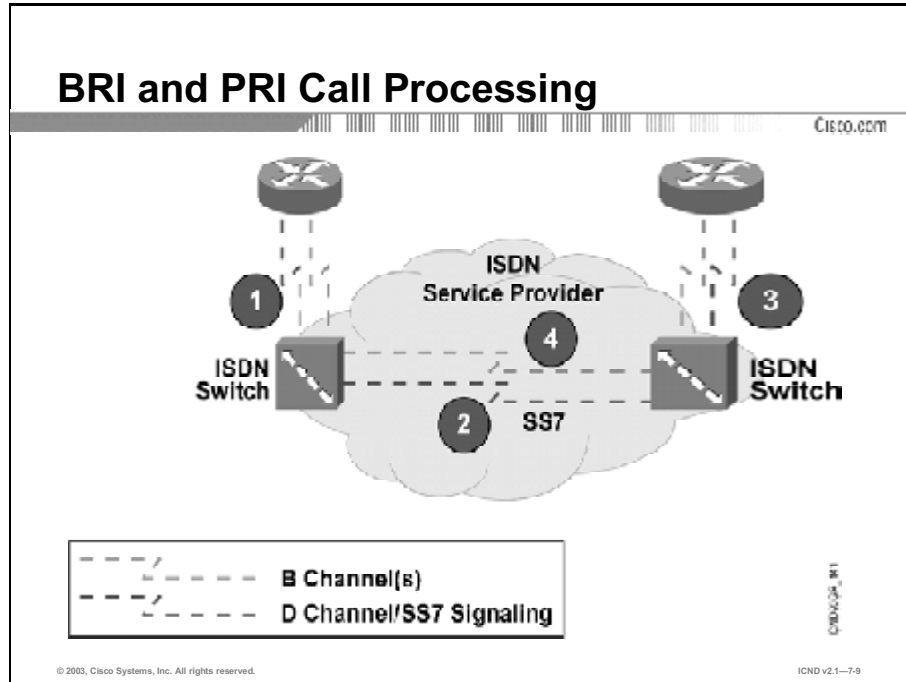
The D channel carries signaling information (call setup) to control calls on B channels. Traffic over the D channel employs the LAPD data-link protocol level. LAPD is based on High-Level Data Link Control (HDLC).

- **PRI:** In North America and Japan, PRI offers 23 64-kbps B channels and 1 64-kbps D channel (a T1/DS1 facility).

In Europe and much of the rest of the world, PRI offers 30 B channels and a D channel (an E1 facility). PRI uses a data service unit (DSU) and/or channel service unit (CSU) for T1/E1 connection.

# Establishing an ISDN BRI or PRI Call

To establish an ISDN call, the D channel is used between the router and the ISDN switch, and Signaling System 7 (SS7) signaling is used between the switches. This topic describes the process of establishing an ISDN call.



The figure shows the sequence of events that occur during the establishment of a BRI or PRI call, as follows:

1. The D channel between the router and the ISDN switch is always up. When the call is initiated, the called number is sent to the local ISDN switch. The D channel is used for call setup, signaling, and termination; that is, the call control functions.
2. The local switch uses the SS7 signaling protocols to set up a path and pass the called number to the terminating ISDN switch.
3. The far-end ISDN switch signals the destination over the D channel.
4. One B channel is then connected end to end. The other B channel is available to a new conversation or data. Both B channels can be used simultaneously.

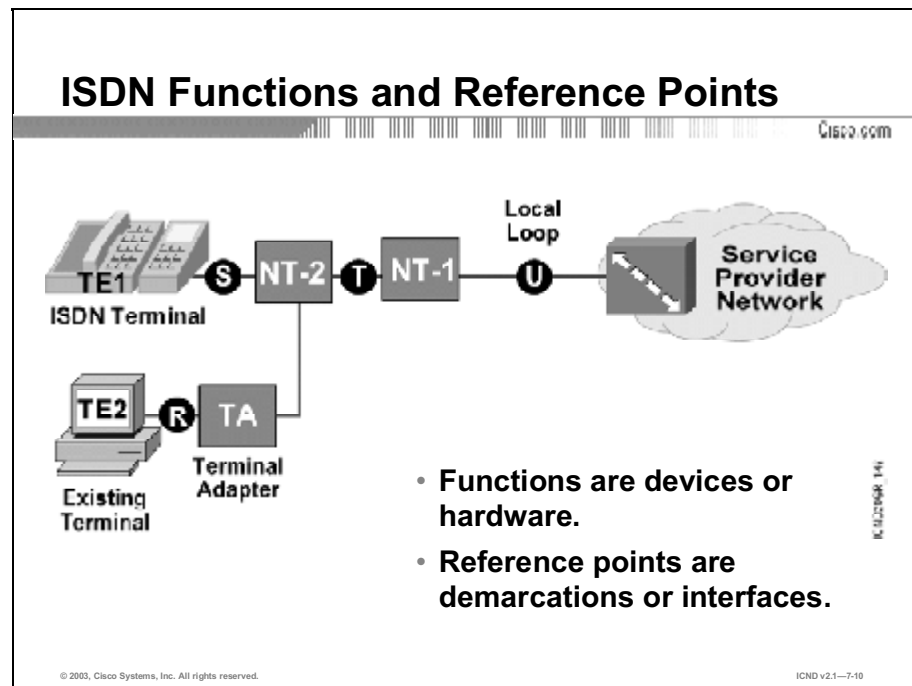
---

**Note** ISDN is the protocol that is used between the endpoints and the local service provider ISDN switch. Within the service provider network, the ISDN call is treated as just a 56- or 64-kbps stream of data and is handled the same as any other stream of data or voice.

---

# ISDN Functions and Reference Points

ISDN functions are implemented as hardware devices while reference points are interfaces between devices. This topic describes the ISDN functions and reference points.



To access the ISDN network, you must use customer premises equipment (CPE) that performs specific functions to connect properly to the ISDN switch. Vendors can create hardware that supports one or more functions because the ISDN standards may be defined in two ways: as a device or as hardware functions. These hardware functions represent a transition point between the reference point interfaces. To select the correct CPE, you must be aware of what functions are available and how the functions relate to each other. The table defines the customer premises ISDN device types and their functions.

| Acronym | Device Type           | Device Function                                                                                                                              |
|---------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| TE1     | Terminal endpoint 1   | Designates a router or ISDN telephone as a device having a native ISDN interface.                                                            |
| NT-2    | Network termination 2 | The point at which all ISDN lines at a customer site are aggregated and switched using a customer switching device. (Seen with an ISDN PBX.) |
| NT-1    | Network termination 1 | Converts the four-wire BRI signals from an S/T interface into two-wire signals of a U interface used by the ISDN digital line.               |
| TE2     | Terminal endpoint 2   | Designates a device such as a PC or router requiring a TA to adapt communication for BRI signals.                                            |
| TA      | Terminal adapter      | Converts EIA/TIA-232, V.35, and other signals into BRI signals.                                                                              |

In Europe, the NT-1 is CPE equipment that is owned by the Post, Telephone, and Telegraph (PTT).

To connect devices that perform specific functions, the devices need to support specific interfaces. Because CPEs can include one or more functions, the interfaces they use to connect

to other devices that support other functions can vary. As a result, the standards do not define interfaces in terms of hardware, but refer to them as reference points. A reference point defines a connection type between two functions. In other words, reference points are a series of specifications that define the connection between specific devices, depending on their function in the end-to-end connection. It is important to understand these interface types because a CPE device such as a router can support different reference types, which could result in the need for additional equipment.

The reference points that affect the customer side of the ISDN connection are as follows:

- **R:** References the point (connection) that is between a non-ISDN compatible device and a terminal adapter.
- **S:** References the points that connect into the NT-2, or customer switching device. It is the interface that enables calls between the various types of CPE.
- **T:** Electrically identical to the S interface, it references the outbound connection from the NT-2 to the ISDN network.

---

|             |                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The electrical similarities between the S and T references why some interfaces are labeled S/T interfaces, because although they perform totally different functions, the port is electrically the same and can be used for either function. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

- **U:** References the connection between the NT-1 and the ISDN network owned by the telephone company.

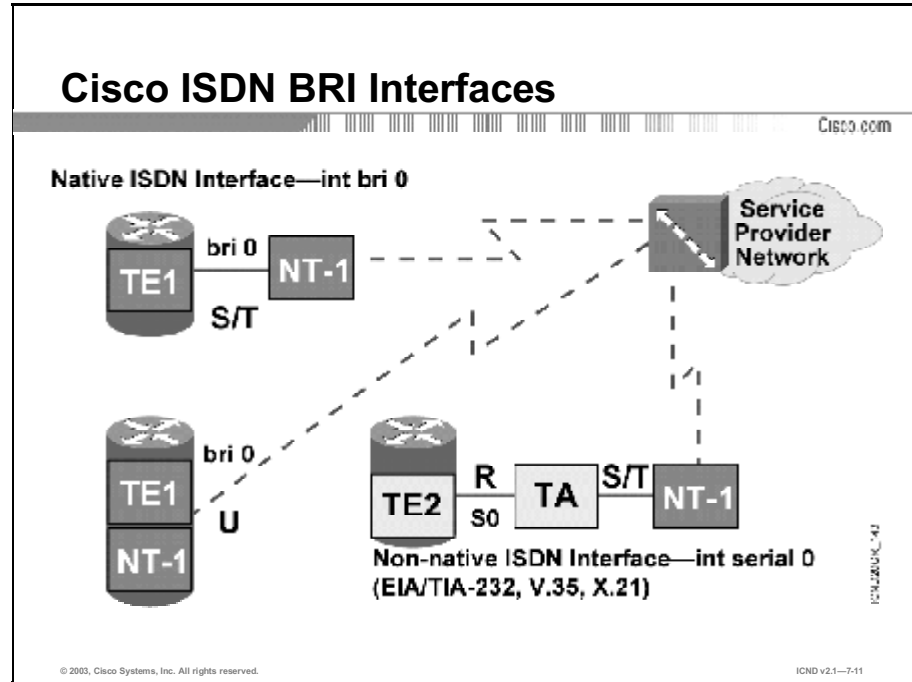
---

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | In the United States, the end user is required to provide the NT-1. In Europe and other countries, the telephone company provides the NT-1 function and presents an S/T interface to the customer. In these configurations, the customer is not required to supply a separate NT-1 device or integrated NT-1 function in the terminal device. Be sure to order your equipment such as router ISDN modules and interfaces accordingly. |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

# Determining the Router ISDN Interface

You can physically configure Cisco routers with different ISDN options, which dictate what additional external equipment, if any, is needed to run ISDN. This topic describes the different ISDN interfaces.



Not all Cisco routers include a native ISDN terminal, nor do all of them include interfaces for the same reference point; therefore, you must evaluate each router carefully. To select a Cisco router with the appropriate ISDN interface, complete the following:

1. Determine whether the router supports ISDN BRI. Look on the back of your router for one of the following:
  - If you see a connector labeled “BRI,” you already have an ISDN BRI. With a native ISDN interface already built in, your router is a TE1. If your router has a U interface, it also has a built-in NT-1.
  - If you do not see a connector labeled “BRI,” and you have a nonmodular router (a fixed-configuration router that does not permit the replacement or addition of interfaces), then you need to use an existing serial interface. With non-native ISDN interfaces such as serial interfaces, you need to obtain an external terminal adapter (TA) device and attach it to the serial interface to provide BRI connectivity. If you have a modular router it may be possible to upgrade to a native ISDN interface providing you have an available slot.
2. Determine whether you or the service provider supplies NT-1. An NT-1 terminates the local loop to the central office (CO) of your ISDN service provider. In the United States, for example, the NT-1 is the responsibility of the customer. In Europe, the service provider typically supplies the NT-1.
3. If you must supply the NT-1, make sure your router has a U interface; if not, you must purchase an external NT-1.

---

**Caution**      Never connect a router with a U interface into an NT-1. It will most likely damage the interface.

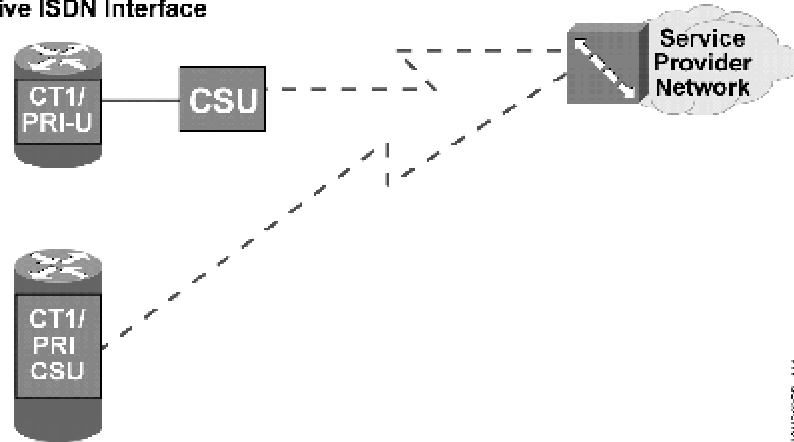
---



## Cisco ISDN PRI Interfaces

Cisco.com

### Native ISDN Interface



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-12

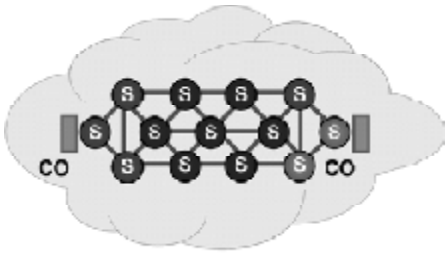
PRI technology is somewhat simpler than BRI. The wiring is not multipoint; there is only a straight connection between the CSU/DSU and the PRI interface.

Multipoint refers to the ability to have multiple ISDN devices connected to the network, all of which have access to the ISDN network. As a result, there is arbitration at Layer 1 and Layer 2, allowing multiple devices to access the network without collisions or interruptions between devices that need to share the ISDN network. PRI does not require this arbitration.

# ISDN Switch Types

You must configure your router to identify the type of switch it will be communicating with, which depends in part on the country the switch is in. This topic describes the different types of ISDN switches.

## ISDN Switch Types



- Many providers use many different switch types.



- Services vary by region and country.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—7-13

ISDN service providers use a variety of different switch types for their ISDN services. Services offered by the national PTT or other carriers vary considerably from country to country or region to region. Just like modems, each switch type operates slightly differently, and has a specific set of call setup requirements. As a result, before you can connect your router to an ISDN service, you must be aware of the switch types that are used at the CO. You must specify this information during router configuration so the router can place ISDN network-level calls and send data. Following is a sample of countries and the ISDN switch types that you are likely to encounter in your provider ISDN cloud.

| Country                  | Switch Type                                  |
|--------------------------|----------------------------------------------|
| United States and Canada | AT&T 5ESS and 4ESS; Northern Telecom DMS-100 |
| France                   | VN2, VN3                                     |
| Japan                    | NTT                                          |
| United Kingdom           | Net3 and Net5                                |
| Europe                   | Net3                                         |

Some service providers program their switches to emulate another switch type. Therefore, it might be necessary to configure a router to match the emulated switch type for proper operation.

In addition to learning about the switch type that your service provider is using, you may also need to know what service profile identifiers (SPIDs) are assigned to your connection. In many

cases, such as when configuring the router to connect to a DMS-100, you will need to input the SPIDs.

SPIDs are a series of characters, which can look like telephone numbers, that identify you to the switch at the CO. After it is identified, the switch links the services you ordered to the connection. Remember, ISDN is typically used for dialup connectivity. The SPIDs are processed during each call-setup operation.

# Configuring ISDN BRI

To enable ISDN BRI operation, you use **isdn switch-type** and the **isdn spid** command. This topic describes the key ISDN-specific commands for enabling an ISDN BRI interface.

## Configuring ISDN BRI



### Step 1: Specify the ISDN switch type.

```
Router(config)#isdn switch-type switch-type
```

```
Router(config-if)#isdn switch-type switch-type
```

- The command specifies the type of ISDN switch with which the router communicates.
- Other configuration requirements vary for specific providers.

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—7-14

Before using ISDN BRI, you must define the **isdn switch-type** global or interface command to specify the ISDN switch to which the router connects. For ISDN BRI service, example switch types are shown in the table.

| Switch Type         | Description                                       |
|---------------------|---------------------------------------------------|
| <i>basic-5ess</i>   | AT&T basic rate switches (USA)                    |
| <i>basic-dms100</i> | Northern Telecom DMS-100 (North America)          |
| <i>basic-nil</i>    | National ISDN-1 (North America)                   |
| <i>basic-ts013</i>  | TS013 switches (Australia)                        |
| <i>basic-net3</i>   | Switch type for Net3 in United Kingdom and Europe |
| <i>ntt</i>          | NTT ISDN switch (Japan)                           |
| <i>none</i>         | No specific switch specified                      |

---

**Note** Configuring the **isdn switch-type** command globally will specify the ISDN switch type for all ISDN interfaces not specifically assigned a switch type.

---

---

**Note** After you configure the router for the correct ISDN switch type, you must restart the router for the setting to become effective.

---

## Configuring ISDN BRI (Cont.)

Cisco.com

### Step 2: (Optional) Setting SPIDs

```
Router(config-if)#isdn spid1 spid-number [ldn]
```

- Sets a B channel SPID required by many service providers

```
Router(config-if)#isdn spid2 spid-number [ldn]
```

- Sets a SPID for the second B channel

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-15

When your ISDN service is installed, the service provider will give you information about your connection. Depending on the switch type used, you may be given two numbers, referred to as the SPIDs. Depending on the switch type, you may need to add these to your configuration. For example, the National ISDN-1 and DMS-100 ISDN switches require SPIDs to be configured, but the AT&T 5ESS switch does not.

The format of the SPIDs can vary depending on the ISDN switch type and specific provider requirements.

Use the **isdn spid1** and **isdn spid2** commands to specify the SPID required to access the ISDN network when your router makes its call to the local ISDN exchange.

| isdn spid1 and isdn spid2<br>Command Parameters | Description                                                                                                                                                         |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>spid-number</i>                              | Number identifying the service to which you have subscribed. The ISDN service provider assigns this value.                                                          |
| <i>ldn</i>                                      | (Optional.) Local dial number. This number must match the called-party information coming in from the ISDN switch in order to use both B channels on most switches. |

# Configuring ISDN PRI

To enable ISDN PRI, use the **pri-group** command. This topic describes the key ISDN-specific commands for enabling an ISDN PRI interface.

## Configuring ISDN PRI

### Step 1: Specify the ISDN switch type.

```
Router(config)#isdn switch-type switch-type
```

### Step 2: Select the controller.

```
Router(config)#controller controller slot/port
```

### Step 3: Establish the interface port to function as PRI .

```
Router(config-controller)#pri-group timeslots range
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-16

The table shows the switch types available for ISDN PRI configuration.

| Switch Type           | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| <i>primary-5ess</i>   | AT&T basic rate switches (USA)                                |
| <i>primary-dms100</i> | Northern Telecom DMS-100 (North America)                      |
| <i>primary-ni</i>     | National ISDN (North America)                                 |
| <i>primary-net5</i>   | Switch type for Net5 in United Kingdom, Europe, and Australia |
| <i>primary-ntt</i>    | NTT ISDN switch (Japan)                                       |

|             |                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | You can configure the ISDN switch type in interface configuration mode if you need to override the global values. |
|-------------|-------------------------------------------------------------------------------------------------------------------|

The procedure outlined in the table describes how to configure a router for ISDN PRI for T1:

| Step | Action                                                                                                                         | Notes                                                                                                                                                                                                                                         |
|------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the ISDN switch type specified by the telephone company.<br><br>Router(config)# <b>isdn switch-type primary-5ess</b> | Selects a switch type of 5ESS.<br><br>Note: An incompatible switch selection configuration can result in failure to make ISDN calls. Reloading the router after changing the switch type is required to make the new configuration effective. |
| 2.   | Begin the configuration of the T1 interface.<br><br>Router(config)# <b>controller t1 3/0</b>                                   | Selects the T1 controller 3/0.<br><br>The <del>slot/port</del> option identifies the T1 controller interface on this router.                                                                                                                  |
| 3.   | Enable PRI on your T1 interface to use all 24 channels.<br><br>Router(config-controller)# <b>pri-group timeslots 1-24</b>      | Establishes the interface port to function as PRI with 23 timeslots designated to operate at a speed of 64 kbps (B channels). Timeslot 23 has the D channel.                                                                                  |

The procedure outlined in the table describes how to configure a router for ISDN PRI for E1:

| Step | Action                                                                                                                         | Notes                                                                                                                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the ISDN switch type specified by the telephone company.<br><br>Router(config)# <b>isdn switch-type primary-net5</b> | Selects a switch type of primary-net5.<br><br>Note: An incompatible switch selection configuration can result in failure to make ISDN calls. Reloading the router after changing the switch type is required to make the new configuration effective. |
| 2.   | Begin the configuration of the E1 interface.<br><br>Router(config)# <b>controller e1 3/0</b>                                   | Selects the E1 controller 3/0.<br><br>The <del>slot/port</del> option identifies the E1 controller interface on this router.                                                                                                                          |
| 3.   | Enable PRI on your E1 interface to use all 31 channels.<br><br>Router(config-controller)# <b>pri-group timeslots 1-31</b>      | Establishes the interface port to function as PRI with 31 timeslots. Timeslot 15 has the D channel.                                                                                                                                                   |

|             |                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Although E1 supports 32 channels, the first channel is used for framing and synchronization. Therefore, only 31 E1 channels carry information. |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|

# ISDN PRI Examples

Cisco.com

## T1 Sample Configuration

```
Router(config)#controller T1 3/0
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#pri-group timeslots 1-24

Router(config-controller)#interface Serial3/0:23
Router(config-if)#isdn switch-type primary-5ess
Router(config-if)#no cdp enable
```

## E1 Sample Configuration

```
Router(config)#controller E1 3/0
Router(config-controller)# framing crc4
Router(config-controller)# linecode hdb3
Router(config-controller)# pri-group timeslots 1-31

Router(config-controller)#interface Serial3/0:15
Router(config-if)# isdn switch-type primary-net5
Router(config-if)# no cdp enable
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-17

The example demonstrates the sequence of commands you would enter to configure a router for ISDN PRI with the following characteristics:

- Select the E1 or T1 controller 3/0 line code and framing for the controller.
- Enable PRI on your controller interface to use all of the selected range of channels, for T1 channels 1 through 24 and for E1 channels 1 through 31.
- The ISDN switch type is selected to match the service provider network.



# Verifying the ISDN Configuration

Use **show** commands to verify that your ISDN configuration is functioning properly. This topic describes how to verify your ISDN configuration.

## Verifying the ISDN Configuration



```
Router#show isdn active
```

- Displays current call information

```
Router#show interfaces bri0
```

- Displays statistics for the BRI interface configured on the router

```
Router#show isdn status
```

- Displays the status of an ISDN connection

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—7-18

Use the following commands to verify the basic ISDN configuration.

| Command                           | Description                                                                                                                                                                                                                                               |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show isdn active</code>     | Displays current call information, including called number, the time until the call is disconnected, AOC <sup>1</sup> charging units used during the call, and whether the AOC information is provided during calls or at end of calls.                   |
| <code>show interfaces bri0</code> | Displays statistics for the BRI interface configured on the router.                                                                                                                                                                                       |
| <code>show isdn status</code>     | Ensures that the router is properly communicating with the ISDN switch. In the output, verify that Layer 1 status is ACTIVE, and that the Layer 2 status state MULTIPLE_FRAME_ESTABLISHED appears. This command also displays the number of active calls. |

<sup>1</sup>AOC = advice of charge

# Troubleshooting the ISDN Configuration

You can use **debug** commands to troubleshoot your ISDN configuration. This topic describes how to use **debug** commands to troubleshoot ISDN.

## Troubleshooting the ISDN Configuration



Router#debug isdn q921

- Shows ISDN Layer 2 messages

Router#debug isdn q931

- Shows ISDN call setup and teardown activity (Layer 3)

Router#debug ppp authentication

- Displays the PPP authentication protocol messages

Router#debug ppp negotiation

- Displays information on PPP link establishment

Router#debug ppp error

- Displays protocol errors associated with PPP

© 2003, Cisco Systems, Inc. All rights reserved.ICND v2.1—7-19

Use the following commands to debug and troubleshoot the ISDN configuration.

| Command                         | Description                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>debug isdn q931</b>          | Shows call setup and teardown of the ISDN network connection (Layer 3).                                                                                                                                                                                              |
| <b>debug isdn q921</b>          | Shows data-link layer messages (Layer 2) on the D channel between the router and the ISDN switch. Use this debug if the <b>show isdn status</b> command does not display Layer 1 and Layer 2 up.                                                                     |
| <b>debug ppp negotiation</b>    | Displays information on PPP traffic and exchanges while negotiating the PPP components including LCP <sup>1</sup> , authentication, and NCP <sup>2</sup> . A successful PPP negotiation will first open the LCP state, then authenticate, and finally negotiate NCP. |
| <b>debug ppp authentication</b> | Displays the PPP authentication protocol messages, including CHAP <sup>3</sup> packet exchanges and PAP <sup>4</sup> exchanges.                                                                                                                                      |
| <b>debug ppp error</b>          | Displays protocol errors and error statistics associated with PPP connection negotiation and operation.                                                                                                                                                              |

<sup>1</sup>LCP = link control protocol

<sup>2</sup>NCP = Network Control Program

<sup>3</sup>CHAP = Challenge Handshake Authentication Protocol

<sup>4</sup>PAP = Password Authentication Protocol

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- ISDN defines a digital architecture that provides integrated voice and data capability using the public switched network.
- ISDN specifies two standard access methods, BRI and PRI.
- To establish an ISDN call, the D channel is used between the routers and switches, and SS7 signaling is used between the switches.
- ISDN functions are hardware devices while reference points are interfaces between devices.
- Cisco devices can be physically configured with different ISDN options, which dictate what additional equipment, if any, is needed to run ISDN.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-20

## Summary (Cont.)

Cisco.com

- You must configure your router to identify the type of switch it will be communicating with, which depends in part on the country that the switch is in.
- To enable ISDN BRI, use the `isdn switch-type` and `isdn spid` commands.
- To enable ISDN PRI, use the `pri-group` command.
- Use `show` commands to verify that your ISDN configuration is functioning properly.
- You can use `debug` commands to troubleshoot your ISDN configuration.

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-21

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides

# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) Which channel is used for ISDN out-of-band signaling?
- A) data
  - B) bearer
  - C) d-signal
  - D) d signal
- Q2) What is the bandwidth capability of a single ISDN B channel in the United States?
- A) 28.8 kbps
  - B) 56 kbps
  - C) 64 kbps
  - D) 128 kbps
- Q3) How many B channels are offered by PRI in North America?
- A) 1
  - B) 2
  - C) 23
  - D) 30
- Q4) With what letter should protocols that cover how switching and signaling should operate begin?
- A) E
  - B) I
  - C) Q
  - D) S
- Q5) What mechanism is used to pass call control information between two ISDN switches?
- A) SS7
  - B) ISDN
  - C) D channel
  - D) B channel

- Q6) What is the primary purpose of the D channel in processing an ISDN call?
- A) to carry data traffic
  - B) to carry voice traffic
  - C) to carry video traffic
  - D) to carry call signaling
- Q7) Which acronym represents a device that converts BRI signals from an S/T interface into a U interface that the ISDN digital line can use?
- A) TA
  - B) TE1
  - C) TE2
  - D) NT-1
- Q8) Which reference point refers to the connection between customer terminal equipment and the NT-2, or customer switching device?
- A) R
  - B) S
  - C) T
  - D) U
- Q9) If your router has a U interface, what does that indicate?
- A) It has a built-in TA.
  - B) It has a built-in TE1.
  - C) It has a built-in BRI.
  - D) It has a built-in NT-1.
- Q10) With non-native ISDN interfaces such as serial interfaces, you need to obtain an external \_\_\_\_\_ device.
- A) TA
  - B) TE1
  - C) TE2
  - D) NT-1
- Q11) Where are ISDN NTT switches used?
- A) USA
  - B) Japan
  - C) France
  - D) Europe

- Q12) What kind of ISDN switch is used in Europe?
- A) Net3
  - B) NTT
  - C) VN2
  - D) DMS-100
- Q13) Which command selects a North American switch for a specific interface?
- A) **Router (config)#isdn switch-type basic-net3**
  - B) **Router (config-if)#isdn switch-type basic-5ess**
  - C) **Router (config-if)#isdn switch-type basic-net3**
  - D) **Router (config)#isdn switch-type basic-dms100**
- Q14) Which two switch types require that you configure SPIDs? (Choose two.)
- A) ntt
  - B) basic-ni1
  - C) basic-net3
  - D) basic-5ess
  - E) basic-dms100
- Q15) Which command specifies a North American switch for a PRI interface?
- A) **Router (config-if)#isdn switch-type basic-5ess**
  - B) **Router (config)#isdn switch-type primary-net3**
  - C) **Router (config-if)#isdn switch-type primary-5ess**
  - D) **Router (config)#isdn switch-type primary-dms100**
- Q16) Which command configures a T1 controller to use the first half of available channels for PRI?
- A) **Router(config)#pri-group timeslots 1-12**
  - B) **Router(config)#pri-group timeslots 13-24**
  - C) **Router(config-controller)#pri-group timeslots 1-12**
  - D) **Router(config-controller)#pri-group timeslots 13-24**
- Q17) Which command displays the status of an ISDN link?
- A) **show status**
  - B) **show dialer**
  - C) **show isdn status**
  - D) **show dialer status**

Q18) Which command displays the status of an ISDN connection?

- A) **show status**
- B) **show dialer**
- C) **show isdn status**
- D) **show dialer status**

Q19) Which command shows Layer 2 messages?

- A) **debug isdn**
- B) **debug q921**
- C) **debug isdn q921**
- D) **debug isdn q931**

Q20) What does the command **debug ppp authentication** do?

- A) shows call setup and teardown
- B) shows data-link layer messages
- C) displays protocol errors and error statistics
- D) displays PAP and CHAP packet exchanges



## Quiz Answer Key

- Q1) D  
**Relates to:** Introducing ISDN
- Q2) C  
**Relates to:** Introducing ISDN
- Q3) C  
**Relates to:** ISDN Standards and Access Methods
- Q4) C  
**Relates to:** ISDN Standards and Access Methods
- Q5) A  
**Relates to:** Establishing an ISDN BRI or PRI Call
- Q6) D  
**Relates to:** Establishing an ISDN BRI or PRI Call
- Q7) D  
**Relates to:** ISDN Functions and Reference Points
- Q8) B  
**Relates to:** ISDN Functions and Reference Points
- Q9) D  
**Relates to:** Determining the Router ISDN Interface
- Q10) A  
**Relates to:** Determining the Router ISDN Interface
- Q11) B  
**Relates to:** ISDN Switch Types
- Q12) A  
**Relates to:** ISDN Switch Types
- Q13) B  
**Relates to:** Configuring ISDN BRI
- Q14) B, E  
**Relates to:** Configuring ISDN BRI
- Q15) C  
**Relates to:** Configuring ISDN PRI
- Q16) C  
**Relates to:** Configuring ISDN PRI
- Q17) B  
**Relates to:** Verifying the ISDN Configuration

Q18) C  
**Relates to:** Verifying the ISDN Configuration

Q19) C  
**Relates to:** Troubleshooting the ISDN Configuration

Q20) D  
**Relates to:** Troubleshooting the ISDN Configuration

# Configuring Dial-on-Demand Routing

---

## Overview

Dial-on-demand routing (DDR) allows two or more Cisco routers to establish a dynamic connection over simple dialup facilities. DDR is used for low-volume, periodic network connections over an ISDN network or the public switched telephone network (PSTN). This lesson explains how to configure DDR using ISDN.

## Relevance

You should know how to configure DDR for those situations where a dedicated WAN link is not possible or desirable.

## Objectives

Upon completing this lesson, you will be able to:

- Configure DDR, given a functioning remote access router and a physical ISDN connection
- Use **show** commands to identify the anomalies in the legacy DDR configurations, given a functioning remote access router and a physical ISDN connection
- Use **debug** commands to identify the anomalies in the legacy DDR configurations, given a functioning remote access router and a physical ISDN connection

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- All knowledge presented in the *Introduction to Cisco Networking Technologies* (INTRO) course

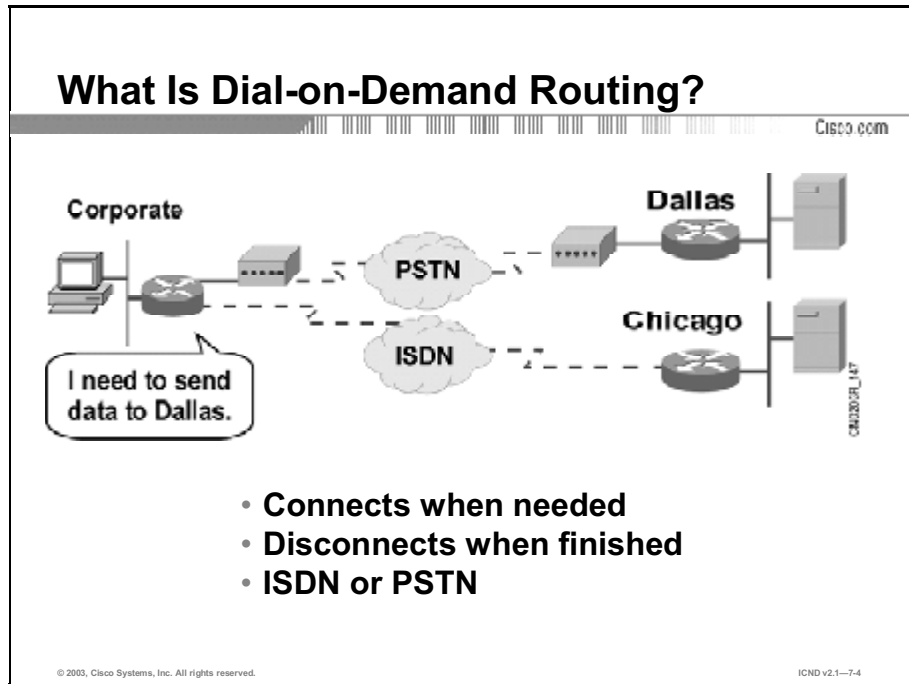
## Outline

The lesson includes these topics:

- Overview
- Introducing DDR
- DDR Operation
- Configuring Legacy DDR
- Defining Static Routes for DDR
- Specifying Interesting Traffic for DDR
- Configuring DDR Dialer Information
- Configuring ISDN PRI and Legacy DDR
- Verifying the DDR Configuration
- Troubleshooting the DDR Configuration
- Summary
- Quiz

# Introducing DDR

Dial-on-demand routing (DDR) refers to a collection of Cisco Systems features that allows two or more Cisco routers to establish a dynamic connection over simple dialup facilities. This topic describes DDR.

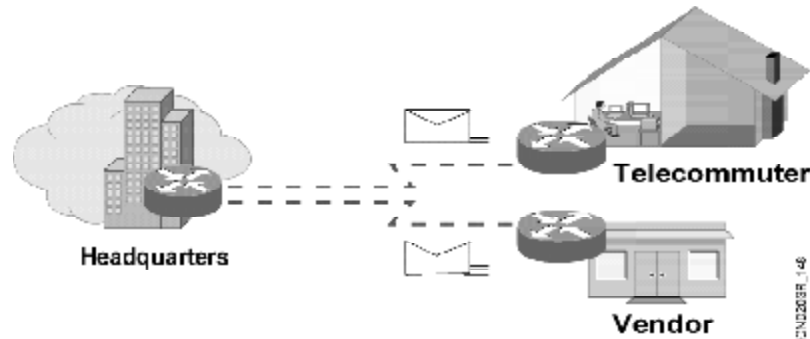


DDR allows two or more Cisco routers to establish a dynamic connection over simple dial-up facilities to route packets and exchange routing updates on an as-needed basis, although static routing is most often used. DDR is used for low-volume, periodic network connections over an ISDN network or the Public Switched Telephone Network (PSTN).

Traditionally, dedicated WAN lines have interconnected networks. DDR addresses the need for periodic network connections over a circuit-switched WAN service. By using WAN connections only on an as-needed basis, DDR can reduce WAN usage costs.

## When to Use DDR

Cisco.com



- **Periodic connections**
- **Small amounts of data**

© 2003, Cisco Systems, Inc. All rights reserved.

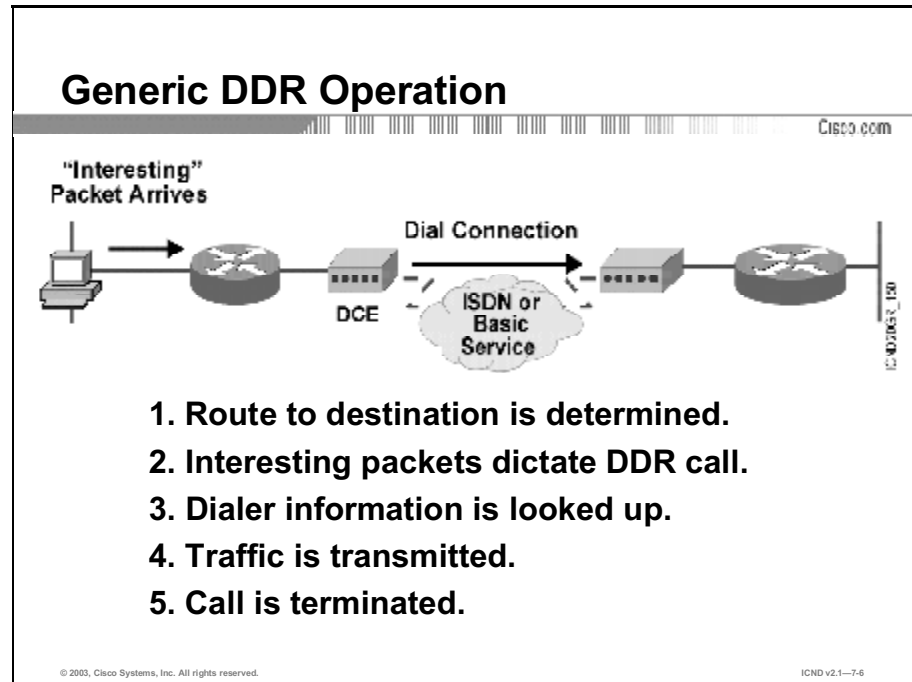
ICND v2.1—7-5

DDR is the process of having a router connect to a PSTN when there is traffic to send, and disconnect when the data transfer is complete. DDR is typically used in the following situations:

- There are telecommuters who need to connect to the company network periodically during the day.
- You have satellite offices that need to send sales transactions or order entry requests to the main computer at the central office (CO).
- As a customer, you want to order products through the automated order system that your vendor has in place.
- Your customers prefer that you send them reports, for example, by e-mail.

# DDR Operation

DDR is triggered by the receipt of traffic that is destined for an interface configured for DDR. If the traffic is “interesting,” a call is initiated. After the interesting traffic has been transmitted, the call is terminated. This topic describes the operation of basic DDR.

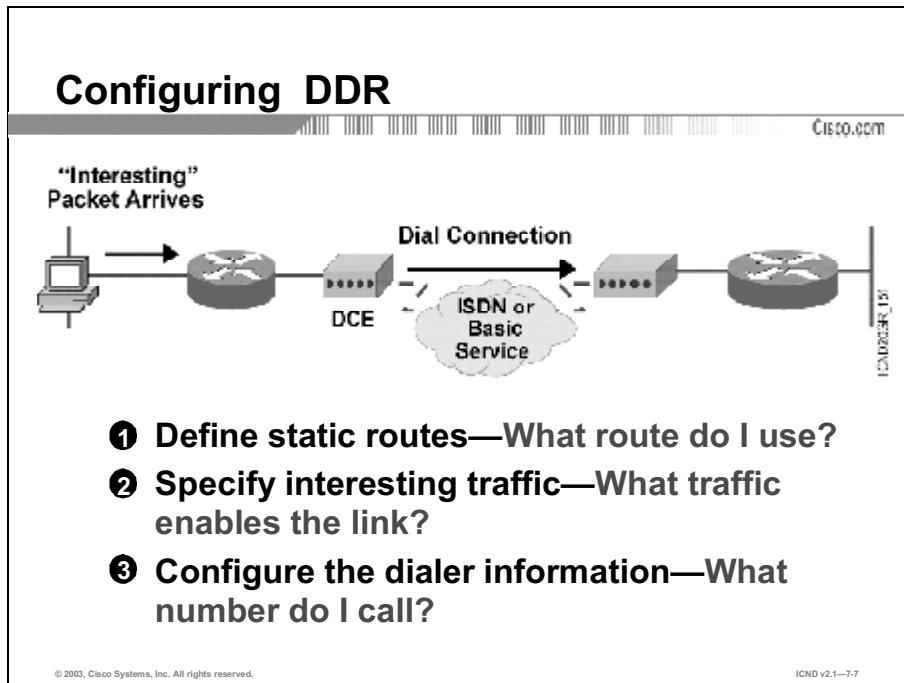


DDR is implemented in Cisco routers in the following steps:

- Step 1** The router receives traffic and does a route table lookup to determine if there is a route to the destination. If so, the outbound interface is identified.
- Step 2** If the outbound interface is configured for DDR, then the router does a lookup to determine if the traffic is “interesting.”  
The administrator, defines interesting traffic. It is any traffic that triggers a call so that the traffic can be transferred.
- Step 3** The router then identifies the next-hop router and locates the dialing instructions in what is called the dialer map.
- Step 4** The router then checks to see if the dialer map is in use; that is, if the interface is currently connected to the remote destination.  
If the interface is currently connected to the desired remote destination, the traffic is sent and, if the packet is interesting, the idle timer is reset. It should be noted that when a connection is established, any traffic to that destination will be permitted; however, only interesting traffic would reset the idle timer.  
If the interface is not currently connected to the remote destination, the router, which is attached to a Basic Rate Interface (BRI), will send call-setup information using the data (D) channel.  
After the link is enabled, the router transmits both interesting and uninteresting traffic. Uninteresting traffic can include data and routing updates.
- Step 5** When no more interesting traffic is transmitted over the link, an idle timer starts. The call is disconnected after no interesting traffic is seen for the duration of the idle timeout period.

# Configuring Legacy DDR

Legacy DDR is a term that is used to define a very basic DDR configuration in which a single set of dialer parameters is applied to an interface. If you need multiple unique dialer configurations on one interface, consider using dialer profiles. To configure DDR, first define the static routes, then specify interesting traffic, and finally configure the dialer information. This topic describes the DDR configuration steps.



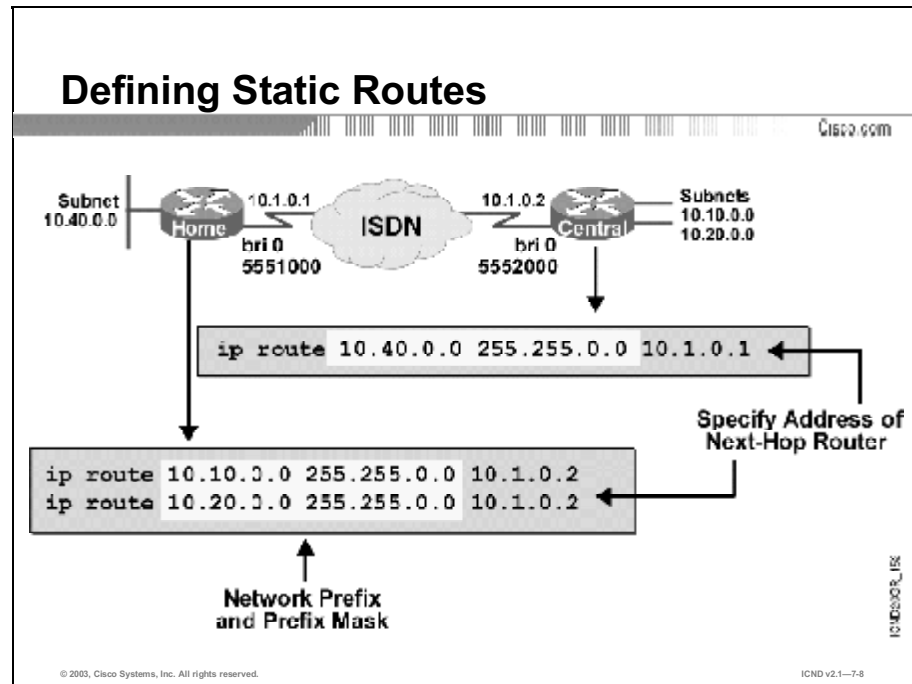
To configure DDR, perform the following steps:

- Step 1** Define static routes. Ask: What route do I take to get to the destination?
- Step 2** Specify interesting traffic. Ask: *What traffic type should enable the link?*
- Step 3** Configure the dialer information. Ask: *What number do I call to get to the next-hop router and what service parameters do I use for the call?*



# Defining Static Routes for DDR

Use static routes across a DDR link so that the number is not dialed to support dynamic routing updates. This topic describes how to define static routes for DDR.



To forward traffic, routers must know what route to use for a given destination. When a dynamic routing protocol is used across a DDR connection, it causes the DDR interface to dial the remote sites for every routing update or “hello” message, if these packets are defined as interesting traffic. To prevent the frequent or even constant activation of the DDR link that is necessary to support dynamic routing protocols across the link, you must manually configure the routes statically. The static route command for IP, for example, is as follows:

```
Router(config)#ip route prefix mask {address | interface} [distance]
[permanent]
```

The table describes the **ip route** parameters.

| ip route Command Parameters | Description                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------|
| <i>prefix</i>               | IP route prefix for the destination.                                                       |
| <i>mask</i>                 | Prefix mask for the destination.                                                           |
| <i>address</i>              | IP address of the next hop that can be used to reach that network.                         |
| <i>interface</i>            | Network interface to use.                                                                  |
| <i>distance</i>             | (Optional) An administrative distance.                                                     |
| <b>permanent</b>            | (Optional) Specifies that the route will not be removed, even if the interface shuts down. |

When configuring static routes, keep in mind the following considerations:

- All participating routers must have static routes defined so that they can reach the remote networks. This requirement is necessary because static routes replace routing updates.
- To reduce the number of static route entries, you can define a summarized or default static route.

# Specifying Interesting Traffic for DDR

DDR calls are triggered by “interesting” traffic, which can be defined based on protocol, source address, destination address, or a variety of other criteria. This topic describes how to define interesting DDR traffic.

## Specifying Interesting Traffic

Cisco.com

```
dialer-list 1 protocol ip permit
```

- Any IP traffic will initiate the link without access lists.

```
dialer-list 1 protocol ip list 101
```

```
access-list 101 deny tcp any any eq ftp
access-list 101 deny tcp any any eq telnet
access-list 101 permit ip any any
```

Denies FTP  
Denies Telnet

- Any IP traffic, except FTP and Telnet, will initiate the linking.
- Using access lists gives finer control.

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—7-9

Identify the protocol packets designated as interesting that will trigger a DDR call. Interesting packets are designated by the administrator and can be defined by a variety of criteria, such as protocol type or addresses for source or destination hosts. Use the **dialer-list** global command to identify interesting traffic. The command syntax is as follows:

```
Router(config)#dialer-list dialer-group protocol protocol-name
{permit | deny} list access-list-number}
```

The table describes the **dialer-list** parameters.

| dialer-list protocol<br>Command Parameters | Description                                                                                                                                                                                                                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>dialer-group</i>                        | Number that maps the dialer list to an interface.                                                                                                                                                                                                                                      |
| <i>protocol-name</i>                       | Specifies the protocol for interesting packets to be considered for DDR; choices include IP, IPX <sup>1</sup> , AppleTalk, DECnet, and VINES <sup>2</sup> .                                                                                                                            |
| <b>permit</b>   <b>deny</b>                | Specifically permits or denies a protocol for DDR.                                                                                                                                                                                                                                     |
| <b>list</b>                                | The <b>list</b> keyword, along with an access list number, assigns an access list to the dialer group. The access list contains the interesting traffic definition. Use an access list to create the interesting traffic definition if you want finer granularity of protocol choices. |

<sup>1</sup>IPX = Internetwork Packet Exchange

<sup>2</sup>VINES = Virtual Integrated Network Service

---

**Note**      If you use the **dialer-list 1 protocol ip permit** command without any further qualification, you will allow all IP traffic to trigger a call.

---

# Configuring DDR Dialer Information

Use the **dialer-group** and **dialer map** commands on an interface to associate a port and dialer-string with a dial list. This topic describes how to configure dialer information for DDR.

## Configuring the Dialer Information

```
hostname Home
!
isdn switch-type basic-5ess
!
username central password cisco
interface BRI0
 ip address 10.1.0.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 180
 dialer map ip 10.1.0.2 name Central 5552000
 dialer-group 1
 no fair-queue
 ppp authentication chap
!
router rip
 network 10.0.0.0
!
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
!
dialer-list 1 protocol ip permit
```

• Applies rules defined by dialer-list to individual interfaces

Both Values Must Match

© 2003, Cisco Systems, Inc. All rights reserved. ICND v2.1—7-10

Perform the following steps to configure the dialer information on a given physical interface:

**Step 1** Select the physical interface that you use as the dial-up line.

**Step 2** Configure the network address for the interface; for example:

```
Router(config-if)#ip address ip-address mask
```

**Step 3** Configure the encapsulation type. If configuring PPP, for example, use this:

```
Router(config-if)#encapsulation ppp
```

Also configure PPP authentication. In this case, the **ppp authentication chap** command is used to specify Challenge Handshake Authentication Protocol (CHAP) authentication for this interface.

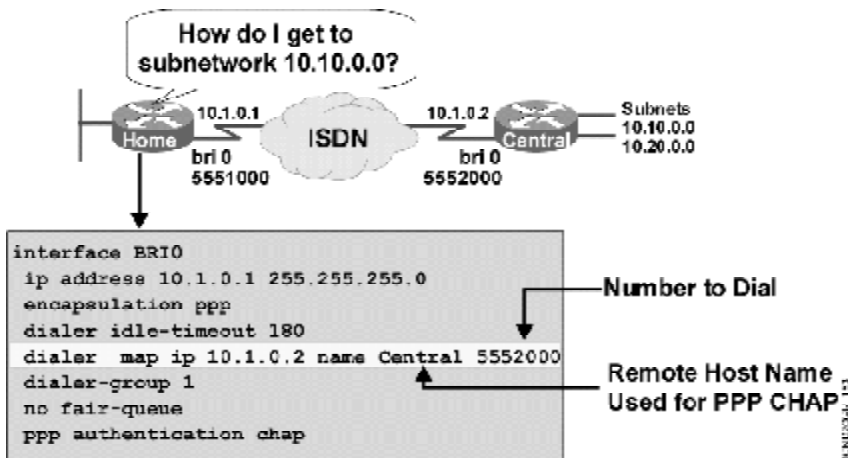
**Step 4** Bind the traffic definition to an interface by linking the interesting traffic definition that you created in Step 1 to the interface.

```
Router(config-if)# dialer-group group-number
```

In the command, *group-number* specifies the number of the dialer group to which the interface belongs. The group number can be an integer from 1 to 10. This number must match the **dialer-list group-number**. Each interface can have only one dialer group, but the same dialer list (using the **dialer-group** command) can be assigned to multiple interfaces.

## Configuring the Dialer Information (Cont.)

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-11

Define one or more dial-on-demand numbers to reach one or more destinations for a particular interface, as follows:

```
Router(config-if)#dialer map protocol next-hop-address [name
hostname] [speed 56 | 64] [broadcast] dialer-string
```

The table describes the **dialer map** parameters.

| dialer map<br>Command Parameters | Description                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>protocol</i>                  | IP, IPX, AppleTalk, DECnet, VINES, and others.                                                                                                                                                                                                                                                                         |
| <i>next-hop-address</i>          | Address of the next-hop router.                                                                                                                                                                                                                                                                                        |
| <b>name</b> <i>hostname</i>      | Host name of the remote device. This name is used for PPP authentication or ISDN calls supporting caller ID.                                                                                                                                                                                                           |
| <b>speed</b> 56   64             | Used for ISDN; indicates the link speed, in kbps, to use. The default is 64.                                                                                                                                                                                                                                           |
| <b>broadcast</b>                 | Indicates that broadcasts and multicasts are permitted to be forwarded to this destination (only when the link is enabled by interesting traffic). DDR is nonbroadcast by default, so no update traffic will cross the link unless this is set. This permits the use of dynamic routing protocols over the connection. |
| <i>dialer-string</i>             | Telephone number sent to the device when packets with the specified next-hop address are received.                                                                                                                                                                                                                     |

The **dialer map** command must be used with the **dialer-group** command and its associated access list to initiate dialing.

## Optional Legacy DDR Commands

Cisco.com

```
Router(config-if)#dialer load-threshold load
[outbound | inbound | either]
```

- Establishes the amount of traffic on the link before a second link is enabled

```
Router(config-if)#dialer idle-timeout seconds
```

- Establishes the idle time before disconnect

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-12

You can use the following optional commands with DDR:

- Use the **dialer load-threshold** command (Cisco proprietary) to configure bandwidth on demand by setting the maximum load before the dialer places another call.

The table describes the **dialer load-threshold** parameters.

| dialer load-threshold<br>Command Parameter          | Description                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>load</i>                                         | Interface load (from 1 to 255) beyond which the dialer will initiate another call to the destination. The bandwidth is defined as a ratio of 255, where 255 would be 100 percent of the available bandwidth.                                                           |
| <b>outbound</b>  <br><b>inbound</b>   <b>either</b> | (Optional.) <b>outbound</b> calculates the actual load using outbound traffic only. <b>inbound</b> calculates the actual load using inbound traffic only. <b>either</b> calculates the actual load using combined outbound and inbound loads. The default is outbound. |

- Use the **dialer idle-timeout** *seconds* command to specify the number of idle seconds before a call is disconnected: *seconds* is the number of seconds until a call is disconnected after the last interesting traffic is sent. The default is 120.

## Legacy DDR Configuration Tasks Summarized

Cisco.com

```

hostname Home
!
isdn switch-type basic-5ess
!
username central password cisco
interface BRI0
 ip address 10.1.0.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 180
 dialer map ip 10.1.0.2 name Central 5552000
 dialer-group 1
 no fair-queue
 ppp authentication chap
!
router rip
network 10.0.0.0
!
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
dialer-list 1 protocol ip permit
!

```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-13

The configuration in this figure shows the results when all steps are performed for DDR. Each step is described in the table.

| Step | Action                                                                                                                                                                          | Notes                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure the static route for DDR transmission using the <b>ip route</b> global configuration command.<br><br>Router(config)# <b>ip route</b> 10.10.0.0 255.255.0.0 10.1.0.2   | You can use this command with other routed protocols, such as IPX.                                                                                                                    |
| 2.   | Identify interesting traffic using the <b>dialer-list</b> global command.<br><br>Router(config)# <b>dialer-list</b> 1 protocol ip permit                                        | You can assign access lists to DDR using the list parameter of this command.                                                                                                          |
| 3.   | Select a physical interface as the dial-up line using the <b>interface</b> configuration command.<br><br>Router(config)# <b>interface</b> bri0                                  | After the <b>interface</b> command is entered, the CLI <sup>1</sup> prompt will change from (config)# to (config-if)#.                                                                |
| 4.   | Configure the network address for the interface using the <b>ip address</b> interface configuration command.<br><br>Router(config-if)# <b>ip address</b> 10.1.0.1 255.255.255.0 | Remember, this command configures the address on the source router.                                                                                                                   |
| 5.   | Configure the encapsulation type using the <b>encapsulation</b> interface configuration command.<br><br>Router(config-if)# <b>encapsulation</b> ppp                             | If you are configuring PPP, also configure PPP authentication for security. For example, the <b>ppp authentication chap</b> command specifies CHAP authentication for this interface. |

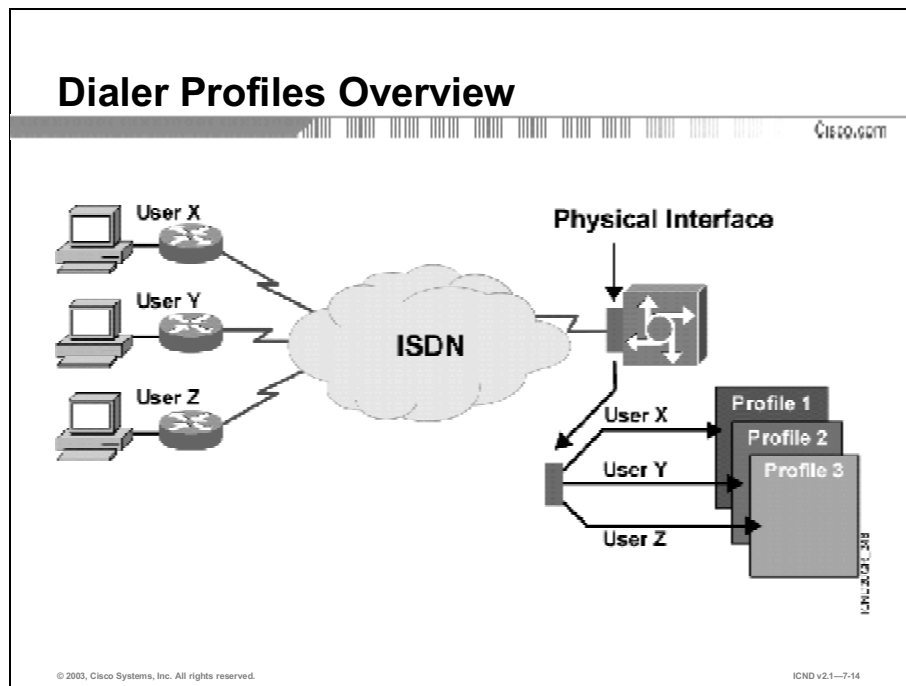


| Step | Action                                                                                                                                                                                                                                                   | Notes                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | Bind the traffic definition to an interface by linking the interesting traffic definition you created in the dialer-list to the interface using the <b>dialer-group</b> interface configuration command.<br><br>Router(config-if)# <b>dialer-group 3</b> | The group number can be an integer from 1 to 10. This number must match the dialer-list group number.<br><br>Each interface can have only one dialer group, but the same dialer list (using the <b>dialer-group</b> command) can be assigned to multiple interfaces. |
| 7.   | Define one or more dial-on-demand numbers to reach one or more destinations for a particular interface using the <b>dialer map</b> interface configuration command.<br><br>Router(config-if)# <b>dialer map ip 10.1.0.2 name Ocoee speed 64 6562054</b>  | Use the <b>dialer map</b> command with the <b>dialer-group</b> command and its associated access list to initiate dialing.                                                                                                                                           |
| 8.   | Exit from interface configuration mode.<br><br>Router(config-if)# <b>exit</b>                                                                                                                                                                            | The command prompt returns to <b>Router#</b> .                                                                                                                                                                                                                       |
| 9.   | Verify the legacy DDR configuration using the <b>show ip route</b> command.<br><br>Router# <b>show ip route</b>                                                                                                                                          | Use the <b>show ip route</b> command to display the routes known to the router, including static and dynamically learned routes.                                                                                                                                     |
| 10.  | Verify that you entered the parameters without error using the <b>show running-config</b> command.<br><br>Router# <b>show running-config</b>                                                                                                             | Use the <b>show running-config</b> command to display the current running configuration. Look at the parameters you configured, looking for typographical errors and incorrect numerical values.                                                                     |

<sup>1</sup>CLI = command-line interface

# Configuring ISDN PRI and Legacy DDR

To configure ISDN Primary Rate Interface (PRI) with legacy DDR, you will configure dialer profiles. This topic shows you how to configure ISDN PRI with legacy DDR.



Dialer profiles separate the “logical” configuration from the interface that is receiving or making calls. Profiles can define encapsulation and access control lists (ACLs), determine minimum or maximum calls, and turn features on or off.

With dialer profiles, the logical and physical configurations are dynamically bound to each other on a per-call basis, which allows physical interfaces to dynamically take on different characteristics based on incoming or outgoing call requirements.

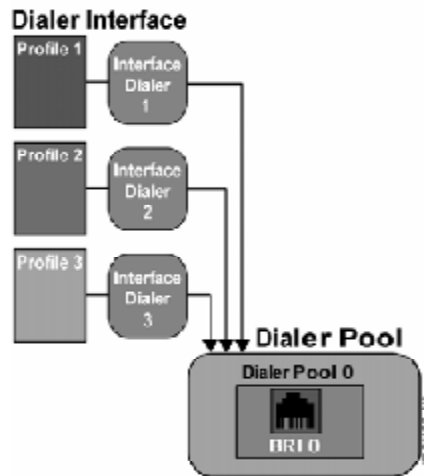
Dialer profiles help users design and deploy complex and scalable circuit-switched internetworks by implementing a new DDR model in Cisco routers and access servers. Dialer profiles separate the logical portion of DDR, such as the network layer, encapsulation, and dialer parameters, from the physical interface that places or receives calls.

Using dialer profiles, you can perform the following tasks:

- Configure bearer (B) channels of an ISDN interface with different IP subnets
- Use different encapsulations of B channels of an ISDN interface
- Set different DDR parameters for B channels of an ISDN interface
- Eliminate the waste of ISDN B channels by letting ISDN BRI interfaces belong to multiple dialer pools

## Dialer Profile Elements

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

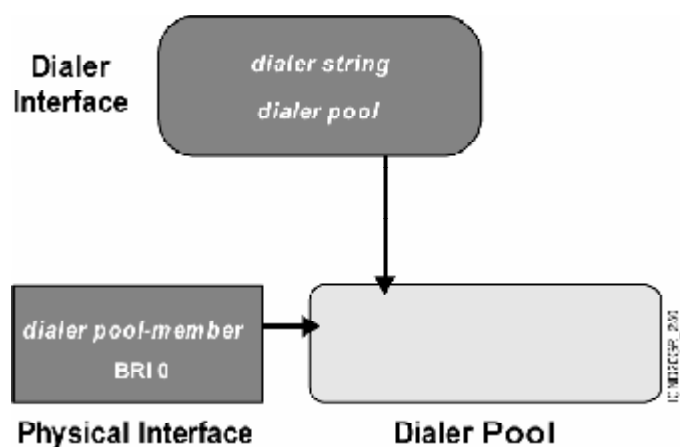
ICND v2.1—7-15

A dialer profile consists of the following elements:

- **Dialer interface:** A logical entity that uses a per-destination dialer profile.
- **Dialer pool:** Each dialer interface references a dialer pool, which is a group of one or more physical interfaces associated with a dialer profile.
- **Physical interfaces:** Interfaces in a dialer pool are configured for encapsulation parameters and to identify the dialer pools to which the interface belongs. Encapsulation type, PPP authentication, and multilink PPP are all configured on the physical interface.

## Dialer Profile Configuration Concepts and Commands

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-16

The configuration commands that create the relationships between the elements of a dialer profile are shown in the figure. The table describes the commands and the configuration mode in which they are used.

| Command                                                                | Description                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>dialer string number</code><br><code>class map class-name</code> | A dialer interface command that specifies the phone number of the destination. The use of the optional keyword <b>class</b> followed by the <b>map class</b> name points to a specific map class and uses the configuration commands of that map class in the call. |
| <code>dialer pool number</code>                                        | A dialer interface command that specifies the pool of physical interfaces available to reach the destination subnetwork. A number between 1 and 255 identifies the pool.                                                                                            |
| <code>dialer pool-member number</code>                                 | An interface configuration command that associates and places a physical interface in a specifically numbered pool.                                                                                                                                                 |

# Configuring Dialer Interfaces

Cisco.com

```
interface dialer1
ip address 10.1.1.1
255.255.255.0
encapsulation ppp
dialer remote-name Smalluser
dialer string 5554540
dialer idle-timer 180
dialer pool 1
dialer-group 1
ppp authentication chap
!
interface dialer2
ip address 10.2.2.1
255.255.255.0
encapsulation ppp
dialer remote-name Mediumuser
dialer string 5551234
dialer idle-timer 180
dialer pool 1
dialer-group 2
```

(cont.)

```
interface dialer3
ip address 10.3.3.1 255.255.255.0
encapsulation ppp
dialer remote-name Poweruser
dialer string 4155554321
dialer idle-timer 300
dialer pool 1
dialer-group 3
```

To configure dialer profiles, perform the following tasks:

- Step 1** Configure one or more dialer interfaces.
- Step 2** Configure a dialer string and optionally a dialer map class to specify different characteristics on a per-call basis.
- Step 3** Configure the physical interfaces and attach them to a dialer pool.

You can configure any number of dialer interfaces for a router. Each dialer interface is the complete configuration for a destination. The **interface dialer** global command creates a dialer interface and enters interface configuration mode.

## Configuring Physical Interfaces

Cisco.com

```
interface bri0
encapsulation ppp
dialer pool-member 1
ppp authentication chap
```

dialer pool 1  
bri0

ICND 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-18

Use the **dialer pool-member** command to assign a physical interface to a dialer pool. You can assign an interface to multiple dialer pools by using this command to specify several dialer pool numbers.

If you have more than one physical interface in the pool, use the **priority** option of the **dialer pool-member** command to set the interface priority within a dialer pool, which is used only when dialing out. You can use a combination of synchronous, serial, BRI, or PRI interfaces with dialer pools.

The table describes the **dialer pool-member** parameters.

| dialer pool-member<br>Command Parameters | Description                                                                                                                                                                                                                                                                                        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>number</b>                            | Specifies the dialer pooling number. This is a decimal value from 1 to 255.                                                                                                                                                                                                                        |
| <b>priority</b> <i>priority</i>          | Sets the priority of the physical interface within the dialer pool. This is a decimal value from 1 to 255. Interfaces with the highest priority number are selected first when dialing out. Use this to determine which interfaces are used the most, or which are reserved for special pool uses. |
| <b>min-link</b> <i>minimum</i>           | Sets the minimum number of ISDN B channels on an interface reserved for this dialer pool. This is a number from 1 to 255 (used for dialer backup).                                                                                                                                                 |
| <b>max-link</b> <i>maximum</i>           | Sets the maximum number of ISDN B channels on an interface reserved for this dialer pool. This is a number from 1 to 255 (used for dialer backup).                                                                                                                                                 |

# Verifying the DDR Configuration

You use **show** commands to display information about DDR configuration. This topic describes how to verify your DDR configuration.

## Verifying DDR and ISDN Operation

Router#ping or telnet

- Triggers a link

Router#show dialer

- Displays current status of the link

Router#show isdn active

- Displays call status while call is in progress

Router#show isdn status

- Displays the status of an ISDN connection

Router#show ip route

- Displays all routes, including static routes

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-18

The table lists the commands to use to verify that DDR is operating correctly.

| Command                 | Description                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ping/telnet</b>      | When you ping or Telnet a remote site (assuming these are not filtered), or when other interesting traffic triggers a link, the router will send a change in link status message to the console.                                                                                                                                                                                                        |
| <b>show dialer</b>      | Lists general diagnostic information about an interface configured for DDR, such as the number of times the dialer string has been successfully reached, and the idle timer and the fast-idle timer values for each B channel. Current call-specific information is also provided, such as the length of the call, and the number and name of the device to which the interface is currently connected. |
| <b>show isdn active</b> | Use this command when using ISDN. It shows that a call is in progress and lists the number called.                                                                                                                                                                                                                                                                                                      |
| <b>show isdn status</b> | Shows the statistics of the ISDN connection.                                                                                                                                                                                                                                                                                                                                                            |
| <b>show ip route</b>    | Displays all routes, including static routes                                                                                                                                                                                                                                                                                                                                                            |

## Verifying Dialer Profiles Operation

Cisco.com

```
NASX#show dialer interface bri0
BRI0 - dialer type = ISDN

Dial String	Successes	Failures	Last called	Last status
5553872	6	0	19 secs	Successful

0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)

Interface bound to profile Dialer0

Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5553872 (system1)

BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle


```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-20

The **show dialer interface BRI** command displays information in the same format as the legacy DDR statistics on incoming and outgoing calls.

In the figure, the message “Dialer state is data link layer up” suggests that the dialer came up properly.

If you see a “physical layer up” message, the line protocol came up but the Network Control Program (NCP) did not.

The source and destination addresses of the packet that initiated the dialing are shown on the “Dial reason” line.



# Troubleshooting the DDR Configuration

You can use **debug** commands to help troubleshoot problems with a DDR configuration. This topic describes how to troubleshoot DDR calls.

## Troubleshooting DDR and ISDN Operation

Router#debug isdn q921

- Shows ISDN Layer 2 messages

Router#debug isdn q931

- Shows ISDN call setup and teardown activity

Router#debug dialer [events | packets]

- Displays DDR debugging information about the packets received on a dialer interface

Router(config-if)#shutdown

- Clears currently established connections from the interface

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-21

The table shows the commands for troubleshooting legacy DDR operation.

| Command                                      | Description                                                                          |
|----------------------------------------------|--------------------------------------------------------------------------------------|
| <code>debug isdn q921</code>                 | Verifies that you have a connection to the ISDN switch.                              |
| <code>debug isdn q931</code>                 | Displays call setup and teardown messages.                                           |
| <code>debug dialer [events   packets]</code> | Displays DDR debugging information about the packets received on a dialer interface. |
| <code>shutdown</code>                        | Administrative shutdown of the interface, will disconnect any call in progress.      |

## debug isdn q921 Example

Cisco.com

```
Router#debug isdn q921

Jan 3 14:52:24.475: ISDN BR0: TX -> INFOc sapi = 0 tei = 64 ns = 5 nr = 2
 i = 0x08010705040288901801837006803631383835
Jan 3 14:52:24.503: ISDN BR0: RX <- RRr sapi = 0 tei = 64 nr = 6
Jan 3 14:52:24.527: ISDN BR0: RX <- INFOc sapi = 0 tei = 64 ns = 2 nr = 6
 i = 0x08018702180189
Jan 3 14:52:24.535: ISDN BR0: TX -> RRr sapi = 0 tei = 64 nr = 3
Jan 3 14:52:24.643: ISDN BR0: RX <- INFOc sapi = 0 tei = 64 ns = 3 nr = 6
 i = 0x08018707
Jan 3 14:52:24.655: ISDN BR0: TX -> RRr sapi = 0 tei = 64 nr = 4
%LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 3 14:52:24.683: ISDN BR0: TX -> INFOc sapi = 0 tei = 64 ns = 6 nr = 4
 i = 0x0801070F
Jan 3 14:52:24.699: ISDN BR0: RX <- RRr sapi = 0 tei = 64 nr = 7
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up
%ISDN-6-CONNECT: Interface BRI0:1 is now connected to 61885 goodie
Jan 3 14:52:34.415: ISDN BR0: RX <- RRp sapi = 0 tei = 64 nr = 7
Jan 3 14:52:34.419: ISDN BR0: TX -> RRf sapi = 0 tei = 64 nr = 4
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1-7-22

The example shows the output from the **debug isdn q921** command for an outgoing call.

In the following lines, the seventh and eighth most significant hexadecimal numbers indicate the type of message. 0x05 indicates a call setup message, 0x02 indicates a call proceeding message, 0x07 indicates a call connect message, and 0x0F indicates a connect ack (acknowledgment) message.

```
Jan 3 14:52:24.475: ISDN BR0: TX -> INFOc sapi = 0 tei = 64 ns =
5 nr = 2
 i =
0x08010705040288901801837006803631383835
Jan 3 14:52:24.527: ISDN BR0: RX <- INFOc sapi = 0 tei = 64 ns =
2 nr = 6
 i = 0x08018702180189
Jan 3 14:52:24.643: ISDN BR0: RX <- INFOc sapi = 0 tei = 64 ns =
3 nr = 6
 i = 0x08018707
Jan 3 14:52:24.683: ISDN BR0: TX -> INFOc sapi = 0 tei = 64 ns =
6 nr = 4
 i = 0x0801070F
```

## debug isdn q931 Examples

Cisco.com

### Call Setup Procedure for Outgoing Call

```
Router#debug isdn q931

TX -> SETUP pd = 8 callref = 0x04
Bearer Capability i = 0x8890
Channel ID i = 0x83
Called Party Number i = 0x80, '41555121202'
RX <- CALL_PROC pd = 8 callref = 0x84
Channel ID i = 0x89
RX <- CONNECT pd = 8 callref = 0x84
TX -> CONNECT_ACK pd = 8 callref = 0x04....
```

### Call Setup Procedure for Incoming Call

```
Router#debug isdn q931

RX <- SETUP pd = 8 callref = 0x06
Bearer Capability i = 0x8890
Channel ID i = 0x89
Calling Party Number i = 0x0083, '81012345678902'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-23

The example shows output from the **debug isdn q931** command of a call setup procedure for an outgoing call and an incoming call.

## debug dialer Examples

Cisco.com

```
Router#debug dialer events
```

```
Dialing cause: Serial0: ip (s=172.16.1.111 d=172.16.2.22)
```

```
Router#debug dialer packets
```

```
BRI0: ip (s=10.1.1.8, d=10.1.1.1), 100 bytes, interesting (ip PERMIT)
```

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-24

When DDR is enabled on the interface, information concerning the cause of any call (called the *dialing cause*) is displayed using the **debug dialer events** command. The following line of output for an IP packet lists the name of the DDR interface and the source and destination addresses of the packet:

```
Dialing cause: Serial0: ip (s=172.16.1.111 d=172.16.2.22)
```

The following is sample output from the **debug dialer packets** command. The message shows the interface type, the type of packet (protocol) being sent, the source and destination addresses, the size of the packet, and the default action for the packet (in this example, PERMIT).

```
BRI0: ip (s=10.1.1.8, d=10.1.1.1), 100 bytes, interesting (ip PERMIT)
```

## Troubleshooting Inbound Calls

Troubleshooting an inbound call starts at the physical layer and works up the protocol stack. The general flow of reasoning looks for answers to the following questions. A “yes” answer to a question takes you to the next question. The **show** or **debug** command used to determine the answer to the question is shown to the right of each question. Be sure to use only one **debug** command at a time during low usage times to avoid overloading the router.

- Did you see the call arrive? (**debug isdn q931**)
- Does the receiving end answer the call? (**debug isdn q931**)
- Does the call complete? (**debug isdn q931**)
- Is data passing across the link? (**show interfaces bri**)
- Is the session established? (PPP or terminal) (**debug ppp [authentication | negotiation]**)

Use the command **debug isdn q931** to watch the q931 signaling messages go back and forth while the router negotiates the ISDN connection.

The following is an example output from a successful connection:

```
Router#debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
 Bearer Capability i = 0x8890
 Channel ID i = 0x89
 Calling Party Number i = 0x0083, \Q5551234'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

The SETUP message indicates that the remote end is initiating a connection. The call reference numbers are maintained as a pair. In this case, the call reference number for the incoming side of the connection is 0x06, while the call reference number of the outbound side of the connection is 0x86. The bearer capability (often referred to as the bearer cap) tells the router what kind of call is coming in. In this case, the connection is type 0x8890. That value indicates “ISDN speed 64 kbps.”

## Troubleshooting Outbound Calls

Troubleshooting an outbound connection starts at the top of the protocol stack. To troubleshoot an outbound connection, answer the following questions. A “yes” answer to a question takes you to the next question. The **show** and **debug** command used to determine the answer to the question is shown to the right of each question. Be sure to use only one **debug** command at a time during low usage times to avoid overloading the router.

- Does DDR initiate a call? (**debug dialer**)
- Does the call make it out to the ISDN network? (**debug isdn q931**)
- Does the remote end answer the call? (**debug isdn q931**)
- Does the call complete? (**debug isdn q931**)
- Is data passing over the link? (**show interfaces**)
- Is the session established? (PPP or terminal) (**debug ppp [authentication | negotiation]**)

To see whether the dialer is trying to make a call to its remote destination, use the **debug dialer events** command.

The following line of **debug dialer events** output for an IP packet lists the name of the DDR interface and the source and destination addresses of the packet:

```
BRI0: Dialing cause ip (s=172.16.1.111 d=172.16.2.22)
```

# Resolving Outbound Call Problems

Cisco.com

| Cause                                                  | Suggested Actions                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------|
| Missing or incorrect "interesting traffic" definitions | Verify the configuration using show running-configuration                 |
| Incorrect interface state                              | Ensure that the interface state is "up/up" (spoofing)                     |
| Misconfigured dialer map                               | Make sure the dialing interface has at least one dialer map statement     |
| Misconfigured dialer profile                           | Make sure the dialer interface is configured with a dialer pool X command |

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-25

The most common reason for outbound call problems is improper configuration. The table describes possible causes of outbound call problems and suggested solutions.

| Possible Cause                                         | Suggested Actions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Missing or incorrect "interesting traffic" definitions | <ul style="list-style-type: none"> <li>■ Using the <b>show running-configuration</b> command, ensure that the interface is configured with a dialer group and that there is a global level dialer list configured with a matching number.</li> <li>■ Ensure that the <b>dialer-list</b> command is configured to permit either an entire protocol or to permit traffic matching an access list.</li> <li>■ Verify that the access list declares packets going across the link to be interesting. One useful test is to use the privileged EXEC command <b>debug ip packet [list number]</b> using the number of the pertinent access list, and then attempt to ping or otherwise send traffic across the link. If the interesting traffic filters have been properly defined, you will see the packets in the debug output. If there is no debug output from this test, then the access list is not matching the packets.</li> </ul> |
| Incorrect interface state                              | Using the <b>show interfaces [interface name]</b> command, ensure that the interface is in the state "up/up (spoofing)."                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Misconfigured dialer map                               | Use the <b>show running-configuration</b> command to ensure that the dialing interface is configured with at least one dialer map statement that points to the protocol address and called number of the remote site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Misconfigured dialer profile                           | <p>Use the <b>show running-configuration</b> command to ensure that the dialer interface is configured with a <b>dialer pool X</b> command and that a dialer interface on the router is configured with a matching dialer pool, member X. If dialer profiles are not properly configured, you may see a debug message such as "Dialer1: Cannot place call, no dialer pool set."</p> <p>Make sure that a dialer string is configured.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **DDR refers to a collection of Cisco features that allows two or more Cisco routers to establish a dynamic connection over simple dialup facilities.**
- **DDR operates by first determining the route to the destination, then, if the traffic is “interesting,” initiating a call.**
- **To configure DDR, first define the static routes, then specify interesting traffic, and finally configure the dialer information.**
- **Use static routes across a DDR link so that the number is not dialed just for routing updates.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-26

## Summary (Cont.)

Cisco.com

- **DDR calls are triggered by “interesting” traffic, which can be defined based on protocol, source address, destination address, or a variety of other criteria.**
- **Use the dialer group and dialer map commands on an interface to associate a port and dialer string with a dial list.**
- **To configure ISDN PRI with legacy DDR, you will configure dialer rotary groups and dialer profiles.**
- **You use show commands to display information about DDR configuration.**
- **You can use debug commands to help troubleshoot problems with a DDR configuration.**

© 2003, Cisco Systems, Inc. All rights reserved.

ICND v2.1—7-27

## References

For additional information, refer to these resources:

- Cisco IOS Configuration Guides
- Cisco IOS Command Reference Guides
- Dialer Solutions Configuration Guide

## Next Steps

After completing this lesson, go to:

- Lab Exercise 7-1: Completing an ISDN BRI Call and Configuring DDR



# Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

- Q1) DDR is best suited to \_\_\_\_\_ volume, \_\_\_\_\_ connections.
- A) low, periodic
  - B) low, constant
  - C) high, periodic
  - D) high, constant
- Q2) What is one benefit that DDR offers?
- A) decreased LAN cost
  - B) decreased WAN cost
  - C) decreased LAN usage
  - D) increased WAN usage
- Q3) What is “interesting” traffic?
- A) any traffic that can be routed via DDR
  - B) any traffic whose destination is through the DDR interface
  - C) any traffic addresses to the router received from the DDR interface
  - D) any traffic that would trigger a DDR call, as defined by the administrator
- Q4) Where are dialing instructions configured?
- A) the dialer map
  - B) the route table
  - C) the dialup map
  - D) the dialer table
- Q5) When you configure DDR and specify “interesting” traffic, what are you specifying?
- A) link the traffic will enable
  - B) traffic type to enable the link
  - C) number to call to get to the next-hop router
  - D) route the traffic takes to get to the destination

- Q6) What is the logical sequence for completing DDR configuration?
- A) Step 1: Configure dialer information.  
Step 2: Define static routes.  
Step 3: Specify interesting traffic.
  - B) Step 1: Define static routes.  
Step 2: Specify interesting traffic.  
Step 3: Configure dialer information.
  - C) Step 1: Specify interesting traffic.  
Step 2: Define static routes.  
Step 3: Configure dialer information.
  - D) Step 1: Define static routes.  
Step 2: Configure dialer information.  
Step 3: Specify interesting traffic.
- Q7) Why are static routes used in a DDR environment?
- A) Dynamic routes require additional configuration.
  - B) Dynamic routing will not work on a DDR connection.
  - C) Static routes allow the router to make a better routing decision than dynamic routes.
  - D) It is not desirable to have dynamic routing updates activate the DDR connection.
- Q8) What does the command **ip route 10.30.0.0 255.255.0.0 10.40.0.5** do?
- A) specifies that packets destined for the 10.40 network be sent to the router on the 10.30 network
  - B) specifies that packets destined for the 10.30 network be sent to any router on the 10.40 network
  - C) specifies that packets destined for the 10.30 network be sent to the device with the address 10.40.0.5
  - D) specifies that packets destined for the 10.40 network be sent to the device with the address 10.40.0.5
- Q9) Which Cisco IOS command identifies interesting traffic for DDR?
- A) **dialer-list**
  - B) **dialer-map**
  - C) **dialer-link**
  - D) **dialer-group**

Q10) Given the following configuration statements, what kind of traffic will trigger a DDR call?

- `dialer-list 1 protocol ip list 101`
- `access-list 101 deny tcp any any eq ftp`
- `access-list 101 deny icmp any any`
- `access-list 101 permit ip any any`

- A) all IP traffic
- B) FTP and ping (Internet Control Message Protocol [ICMP]) traffic
- C) Telnet and ping (ICMP) traffic
- D) all IP traffic except FTP and ping (ICMP)

Q11) Given the command **dialer-list 4**, what does the “4” reference?

- A) dialer map 4
- B) dialer-map 4
- C) dialer-group 4
- D) dialer group 4

Q12) The command **dialer idle-timeout** specifies the number of seconds between which two events?

- A) The DDR call is initiated; the call is terminated.
- B) Interesting traffic is received; the call is initiated.
- C) The last interesting traffic is sent; the call is terminated.
- D) The first interesting traffic is sent; the call is terminated.

Q13) To what do dialer rotary groups allow you to apply a single logical interface configuration?

- A) two ATM PVCs
- B) a set of physical interfaces
- C) a set of loopback interfaces
- D) multiple Frame Relay connections

Q14) Which command is used to enable DDR on an asynchronous interface?

- A) **dialer map**
- B) **dialer caller**
- C) **dialer in-band**
- D) **dialer callback**

- Q15) Which Cisco IOS command lists general diagnostic information about a DDR interface?
- A) **telnet**
  - B) **show dialer**
  - C) **show isdn active**
  - D) **show isdn status**
- Q16) What does the command **show isdn active** do?
- A) initiates a DDR call
  - B) shows the statistics of an ISDN connection
  - C) shows calls in progress and lists the number called
  - D) lists general diagnostic information about ISDN configuration
- Q17) Which Cisco IOS command displays information about the number an interface is calling?
- A) **shutdown**
  - B) **debug dialer**
  - C) **debug isdn q921**
  - D) **debug isdn status**
- Q18) Troubleshooting outbound calls starts at the \_\_\_\_\_ of the protocol stack and troubleshooting inbound calls starts at the \_\_\_\_\_ of the protocol stack.
- A) top, top
  - B) top, bottom
  - C) bottom, top
  - D) bottom, bottom

## Quiz Answer Key

- Q1) A  
**Relates to:** Introducing DDR
- Q2) B  
**Relates to:** Introducing DDR
- Q3) D  
**Relates to:** DDR Operation
- Q4) A  
**Relates to:** DDR Operation
- Q5) B  
**Relates to:** Configuring Legacy DDR
- Q6) B  
**Relates to:** Configuring Legacy DDR
- Q7) D  
**Relates to:** Defining Static Routes for DDR
- Q8) C  
**Relates to:** Defining Static Routes for DDR
- Q9) A  
**Relates to:** Specifying Interesting Traffic for DDR
- Q10) D  
**Relates to:** Specifying Interesting Traffic for DDR
- Q11) C  
**Relates to:** Configuring DDR Dialer Information
- Q12) C  
**Relates to:** Configuring DDR Dialer Information
- Q13) B  
**Relates to:** Configuring ISDN Primary Rate Interface and Legacy DDR
- Q14) C  
**Relates to:** Configuring ISDN Primary Rate Interface and Legacy DDR
- Q15) B  
**Relates to:** Verifying the DDR Configuration
- Q16) C  
**Relates to:** Verifying the DDR Configuration
- Q17) B  
**Relates to:** Troubleshooting the DDR Configuration

Q18) B

**Relates to:** Troubleshooting the DDR Configuration

# Lesson Assessments

---

## Overview

Use the lesson assessments here to test what you learned in this module. The correct answers and solutions are found in the Lesson Assessment Answer Key.

## Outline

This section includes these assessments:

- Lesson Assessment 7-1: Configuring ISDN BRI and PRI
- Lesson Assessment 7-2: Configuring Dial-on-Demand Routing

# Lesson Assessment 7-1: Configuring ISDN BRI and PRI

Complete this quiz to assess what you learned in the lesson.

## Objectives

This quiz tests your knowledge of how to:

- Configure ISDN BRI and ISDN PRI, given a functioning router and a physical ISDN connection
- Use **show** commands to identify the anomalies in the ISDN BRI and PRI configurations, given a functioning router and a physical ISDN connection
- Use **debug** commands to identify the anomalies in the ISDN BRI and PRI configurations, given a functioning remote access router and a physical ISDN connection

## Quiz

Answer these questions:

- Q1) Which statement is true of ISDN?
- A) ISDN carries only data traffic.
  - B) ISDN offers no speed advantage versus regular modem connections.
  - C) ISDN uses analog lines between the provider network and the customer site.
  - D) ISDN uses out-of-band signaling for faster call setup than modem connections.
- Q2) Why is the ISDN D channel used?
- A) to carry data traffic
  - B) to carry voice traffic
  - C) to carry video traffic
  - D) to provide call signaling
- Q3) In Europe, how many B channels does PRI offer?
- A) 1
  - B) 2
  - C) 23
  - D) 30
- Q4) Protocols that recommend telephone network standards begin with what letter?
- A) E
  - B) I
  - C) Q
  - D) S
- Q5) How much bandwidth is available on the B channel with BRI?
- A) 8 kbps
  - B) 16 kbps
  - C) 64 kbps
  - D) 128 kbps



- Q6) The D channel between the router and the ISDN switch is \_\_\_\_\_.  
A) always up  
B) usually up  
C) always down  
D) always on standby
- Q7) What is the purpose of SS7 in establishing an ISDN call?  
A) to pass call control information between the local and terminating routers  
B) to pass call control information between the router and the local ISDN switch  
C) to pass call control information between the terminating router and ISDN switch  
D) to pass call control information between the local and terminating ISDN switches
- Q8) Which acronym represents a device that converts non-native ISDN signals into BRI signals?  
A) TA  
B) TE1  
C) NT-1  
D) NT-2
- Q9) Which reference point refers to the connection between a non-ISDN compatible device and a terminal adapter?  
A) R  
B) S  
C) T  
D) U
- Q10) What kind of device is a TE2?  
A) a device having a native ISDN interface  
B) a device requiring a TA for its BRI signals  
C) a device that converts BRI signals into a form used by the ISDN digital line  
D) a device where all ISDN lines at a customer site are aggregated and switched
- Q11) What does the ISDN T reference point reference?  
A) the outbound connection from the NT-2 to the ISDN network  
B) the points that connect into the NT-2, or customer switching device  
C) the point (connection) between a non-ISDN compatible device and a terminal adapter  
D) the connection between the NT-1 and the ISDN network owned by the telephone company
- Q12) If your router has an interface labeled "BRI," what does that indicate?  
A) that it is a TA  
B) that it is a TE1  
C) that it is an NT-2  
D) that it is an NT-1

- Q13) What type of interface indicates that your router has a built-in NT-1?
- A) U
  - B) S/T
  - C) BRI
  - D) NT-1
- Q14) Where are Net3 switches used?
- A) USA
  - B) Japan
  - C) France
  - D) Europe
- Q15) What is a SPID?
- A) a series of tones that identify you to the switch
  - B) a series of numbers that identify you to the router
  - C) a series of numbers that identify you to the switch
  - D) a series of characters that identify you to the switch
- Q16) Which Cisco IOS command specifies a European switch for a specific interface?
- A) **Router (config)#isdn switch-type basic-net3**
  - B) **Router (config-if)#isdn switch-type basic-5ess**
  - C) **Router (config-if)#isdn switch-type basic-net3**
  - D) **Router (config)#isdn switch-type basic-dms100**
- Q17) Which Cisco IOS command specifies the SPID for the second B channel?
- A) **spid2 77546721**
  - B) **isdn spid2 77546721**
  - C) **isdn spid1 77546721**
  - D) **isdn spidb2 77546721**
- Q18) Which Cisco IOS command specifies an Australian switch for a PRI interface?
- A) **Router (config-if)#isdn switch-type basic-5ess**
  - B) **Router (config)#isdn switch-type primary-net5**
  - C) **Router (config-if)#isdn switch-type primary-5ess**
  - D) **Router (config)#isdn switch-type primary-dms100**
- Q19) Which Cisco IOS command configures a T1 controller to use all available channels for PRI?
- A) **Router(config)#pri-group timeslots 1-12**
  - B) **Router(config)#pri-group timeslots 1-24**
  - C) **Router(config-controller)#pri-group timeslots 1-24**
  - D) **Router(config-controller)#pri-group timeslots 13-24**

- Q20) Which command shows Layer 3 messages?
- A) **debug isdn**
  - B) **debug q921**
  - C) **debug isdn q921**
  - D) **debug isdn q931**
- Q21) What does the command **debug ppp error** do?
- A) shows call setup and teardown
  - B) shows data-link layer messages
  - C) displays protocol errors and error statistics
  - D) displays the PPP authentication protocol messages

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment 7-2: Configuring Dial-on-Demand Routing

Complete this quiz to assess what you learned in the lesson.

## Objectives

This quiz tests your knowledge of how to:

- Configure legacy DDR, given a functioning remote access router and a physical ISDN connection
- Use **show** commands to identify the anomalies in the legacy DDR configurations, given a functioning remote access router and a physical ISDN connection
- Use **debug** commands to identify the anomalies in the legacy DDR configurations, given a functioning remote access router and a physical ISDN connection

## Quiz

Answer these questions:

- Q1) What would be an appropriate scenario for implementing DDR?
- A) corporate staff need dedicated access to an application server
  - B) customers need to upload their complete inventory every hour
  - C) remote offices need minute-by-minute updates from a file server
  - D) remote staff need to connect to the company network occasionally
- Q2) When does DDR use WAN connections?
- A) never
  - B) constantly
  - C) on a scheduled basis
  - D) on an as-needed basis
- Q3) A DDR call is terminated when \_\_\_\_.
- A) no more traffic is sent
  - B) the idle timeout is reset
  - C) more interesting traffic is sent
  - D) the idle timeout passes with no interesting traffic
- Q4) After a DDR link is established, what type of traffic does the router transmit?
- A) interesting
  - B) uninteresting
  - C) routing update
  - D) interesting and uninteresting
- Q5) What is stored in a dialer map?
- A) static routes
  - B) ISDN switch types
  - C) dialing instructions
  - D) interface identifiers

- Q6) What question corresponds to dialer information?
- A) What link should the traffic enable?
  - B) What traffic type should enable the link?
  - C) What number do I call to get to the next-hop router?
  - D) What route does the traffic take to get to the destination?
- Q7) What is the first logical step in configuring DDR?
- A) defining static routes
  - B) identifying interfaces
  - C) specifying interesting traffic
  - D) configuring dialer information
- Q8) Which command specifies that packets destined for an IP address that begins with 10.40 should be sent to the device with the address 10.20.0.3?
- A) **ip route 10.40.0.0 255.0.0.0 10.20.0.3**
  - B) **ip route 10.20.0.2 255.255.0.0 10.40.0.0**
  - C) **ip route 10.40.0.0 255.255.0.0 10.20.0.3**
  - D) **ip route 255.255.0.0 10.40.0.0 10.20.0.3**
- Q9) When a dynamic routing protocol is used across a DDR connection and an access list is not used to define interface interesting traffic, it causes the DDR interface to dial the remote site \_\_\_\_.
- A) for all traffic
  - B) for ICMP traffic
  - C) for routing updates
  - D) every five minutes
- Q10) Given the following configuration statements, what kind of traffic will trigger a DDR call?
- dialer-list 1 protocol ip list 101
  - access-list 101 deny tcp any any eq telnet
  - access-list 101 deny tcp any any eq ftp
  - access-list 101 permit ip any any
- A) all IP traffic
  - B) FTP and Telnet traffic
  - C) all IP traffic except TCP
  - D) all IP traffic except Telnet and FTP
- Q11) Which Cisco IOS command allows all IP traffic to initiate a DDR call without using an access list?
- A) **dialer-list 1 protocol ip deny**
  - B) **dialer-list 1 protocol ip permit**
  - C) **dialer-list 1 protocol ip list 101**
  - D) **dialer-group 1 protocol ip permit**

- Q12) Which Cisco IOS command assigns the same dialer information to multiple interfaces?
- A) **dialer-list**
  - B) **dialer map**
  - C) **dialer-group**
  - D) **dialer interface**
- Q13) What is the purpose of the **dialer map** command?
- A) to associate a dialer list with a dialer group
  - B) to associate dialing instructions with a dialer list
  - C) to specify dialing instructions to a specific address
  - D) to specify dialing instructions for a specific interface
- Q14) Which Cisco IOS command specifies a bandwidth limit beyond which a second DDR link is established?
- A) **dialer map**
  - B) **dialer-group**
  - C) **dialer idle-timeout**
  - D) **dialer load-threshold**
- Q15) Which interface is visible to the upper-layer protocols when using dialer profiles?
- A) null interfaces
  - B) dialer interfaces
  - C) tunnel interfaces
  - D) physical interfaces
- Q16) Which commands can you configure on physical interfaces when using dialer profiles?
- A) **encapsulation ppp, ppp callback, ip address**
  - B) **encapsulation ppp, ppp quality, ppp compression**
  - C) **encapsulation ppp, ppp authentication, multilink ppp**
  - D) **encapsulation ppp, ppp authentication, dialer fast-idle**
- Q17) Why would you use a **ping** or **telnet** command while verifying a DDR configuration?
- A) to generate traffic
  - B) to initiate a DDR call
  - C) to force an inbound call
  - D) to terminate a DDR call
- Q18) What information does the **debug isdn q931** command display?
- A) PPP authentication information
  - B) negotiation of link compression
  - C) call setup and teardown messages
  - D) data being transmitted over a DDR link

- Q19) What types of calls would you logically troubleshoot by starting at the top of the protocol stack?
- A) inbound
  - B) outbound
  - C) uninteresting
  - D) both inbound and outbound

## Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

# Lesson Assessment Answer Key

## Lesson Assessment 7-1: Configuring ISDN BRI and PRI

|      |   |
|------|---|
| Q1)  | D |
| Q2)  | D |
| Q3)  | D |
| Q4)  | A |
| Q5)  | C |
| Q6)  | A |
| Q7)  | D |
| Q8)  | A |
| Q9)  | A |
| Q10) | B |
| Q11) | A |
| Q12) | B |
| Q13) | A |
| Q14) | D |
| Q15) | D |
| Q16) | C |
| Q17) | B |
| Q18) | B |
| Q19) | C |
| Q20) | D |
| Q21) | C |



## Lesson Assessment 7-2: Configuring Dial-on-Demand Routing

- Q1) D
- Q2) D
- Q3) D
- Q4) D
- Q5) C
- Q6) C
- Q7) A
- Q8) C
- Q9) C
- Q10) D
- Q11) B
- Q12) C
- Q13) C
- Q14) D
- Q15) B
- Q16) C
- Q17) B
- Q18) C
- Q19) B



# Course Glossary

---

The Course Glossary for *Interconnecting Cisco Network Devices* (ICND) v2.1 highlights and defines key terms and acronyms used throughout this course. Many of these terms are also described in the Cisco Internetworking Terms and Acronyms resource, available via <http://www.cisco.com>.

| Acronym or Term           | Definition                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.x                     | A set of IEEE standards for the definition of LAN protocols.                                                                                                                                                                                                                                                                                                                                                                           |
| address                   | Data structure or logical convention used to identify a unique entity, such as a particular process or a network device.                                                                                                                                                                                                                                                                                                               |
| address mask              | A bit combination used to describe which part of an address refers to the network or the subnet and which part refers to the host. Sometimes referred to simply as mask.                                                                                                                                                                                                                                                               |
| address resolution        | Generally, a method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network layer (Layer 3) addresses to data-link layer (Layer 2) addresses.                                                                                                                                                                                                                 |
| administrative distance   | Rating of the trustworthiness of a routing information source. Administrative distance often is expressed as a numerical value between 0 and 255. The higher the value, the lower the trustworthiness rating.                                                                                                                                                                                                                          |
| AppleTalk                 | A series of communications protocols designed by Apple Computer consisting of two phases. Phase 1, the earlier version, supports a single physical network that can have only one network number and be in one zone. Phase 2 supports multiple logical networks on a single physical network and allows networks to be in more than one zone.                                                                                          |
| application               | A program that performs a function directly for a user. FTP and Telnet clients are examples of network applications.                                                                                                                                                                                                                                                                                                                   |
| area                      | A logical set of network segments (OSPF-based) and their attached devices. Areas usually are connected to other areas via routers, making up a single autonomous system. See also autonomous system.                                                                                                                                                                                                                                   |
| ARP                       | Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.                                                                                                                                                                                                                                                                                                                         |
| asynchronous transmission | Term describing digital signals that are transmitted without precise clocking. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and the end of each character.                                                                                                |
| ATM                       | Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.                                                     |
| authentication            | In security, the verification of the identity of a person or a process.                                                                                                                                                                                                                                                                                                                                                                |
| autonomous system         | A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA. Sometimes abbreviated as AS.                                                                                                                                                                                           |
| B channel                 | Bearer channel. DS0 time slot that carries analog voice or digital data over ISDN. In ISDN, a full-duplex, 64-kbps channel used to send user data.                                                                                                                                                                                                                                                                                     |
| backbone                  | Part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.                                                                                                                                                                                                                                                                                                         |
| bandwidth                 | The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth. |
| baud                      | Unit of signaling speed equal to the number of discrete signal elements transmitted per second. Baud is synonymous with bits per second (bps) if each signal element represents exactly 1 bit.                                                                                                                                                                                                                                         |
| Bc                        | committed burst. Negotiated tariff metric in Frame Relay internetworks. The maximum amount of data (in bits) that a Frame Relay internetwork is committed to accept and transmit at the CIR.                                                                                                                                                                                                                                           |

| Acronym or Term         | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Be                      | excess burst. Negotiated tariff metric in Frame Relay internetworks. The number of bits that a Frame Relay internetwork attempts to transmit after Bc is accommodated. Be data, in general, is delivered with a lower probability than Bc data because Be data can be marked as DE by the network.                                                                                                                                         |
| BPDU                    | bridge protocol data unit. Spanning Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.                                                                                                                                                                                                                                                                            |
| BRI                     | Basic Rate Interface. ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data.                                                                                                                                                                                                                                                                                            |
| bridge                  | Device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data-link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame.                                                                                                                                   |
| bridge static filtering | The process in which a bridge maintains a filtering database consisting of static entries. Each static entry equates a MAC destination address with a port that can receive frames with this MAC destination address and a set of ports on which the frames can be transmitted. Defined in the IEEE 802.1 standard.                                                                                                                        |
| broadcast               | Data packets that are sent to all nodes on a network. Broadcasts are identified by a broadcast address.                                                                                                                                                                                                                                                                                                                                    |
| broadcast address       | A special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones.                                                                                                                                                                                                                                                                                                 |
| broadcast domain        | Set of all devices that receive broadcast frames originating from any device within the set. Broadcast domains typically are bounded by routers because routers do not forward broadcast frames.                                                                                                                                                                                                                                           |
| broadcast storm         | An undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.                                                                                                                                                                                                                                  |
| burst                   | In data communications, a sequence of signals counted as one unit in accordance with some specific criterion or measure.                                                                                                                                                                                                                                                                                                                   |
| CDP                     | Cisco Discovery Protocol. Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media. |
| CHAP                    | Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.                                                                                                                       |
| CIR                     | committed information rate. The rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. CIR, measured in bits per second, is one of the key negotiated tariff metrics.                                                                                                                                                                                      |
| Cisco IOS               | Cisco Systems software that provides common functionality, scalability, and security for all Cisco products. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while ensuring support for a wide variety of protocols, media, services, and platforms.                                                                                                                                  |
| CO                      | central office. The local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.                                                                                                                                                                                                                                                                             |
| collision               | In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.                                                                                                                                                                                                                                                                                 |
| communications line     | Physical link (such as wire or a telephone circuit) that connects one or more devices to one or more other devices.                                                                                                                                                                                                                                                                                                                        |

| Acronym or Term                   | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| configuration register            | In Cisco routers, a 16-bit, user-configurable value that determines how the router functions during initialization. The configuration register can be stored in hardware or software. In hardware, the bit position is set using a jumper. In software, the bit position is set by specifying a hexadecimal value using configuration commands.                                                                                                                                                     |
| connectionless                    | Term used to describe data transfer without the existence of a virtual circuit.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| connection-oriented               | Term used to describe data transfer that requires the establishment of a virtual circuit.                                                                                                                                                                                                                                                                                                                                                                                                           |
| core router                       | In a packet-switched star topology, a router that is part of the backbone and that serves as the single pipe through which all traffic from peripheral networks must pass on its way to other peripheral networks.                                                                                                                                                                                                                                                                                  |
| CPE                               | customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.                                                                                                                                                                                                             |
| D channel                         | data channel. Full-duplex, 16-kbps (BRI), or 64-kbps (PRI) ISDN channel.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| datagram                          | Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.                                                                                               |
| DCE                               | data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.                                                                                                |
| DDR                               | dial-on-demand routing. Technique whereby a router can automatically initiate and close a circuit-switched session as transmitting stations demand. The router spoofs keepalives so that end stations treat the session as active. DDR permits routing over ISDN or telephone lines using an external ISDN terminal adaptor or modem.                                                                                                                                                               |
| DE                                | discard eligible. If the network is congested, DE traffic can be dropped to ensure the delivery of higher priority traffic.                                                                                                                                                                                                                                                                                                                                                                         |
| dedicated LAN                     | Network segment allocated to a single device. Used in LAN switched network topologies.                                                                                                                                                                                                                                                                                                                                                                                                              |
| default route                     | Routing table entry that is used to direct frames for which a next hop is not explicitly listed in the routing table.                                                                                                                                                                                                                                                                                                                                                                               |
| delay                             | The time between the initiation of a transaction by a sender and the first response received by the sender. Also, the time required to move a packet from source to destination over a given path.                                                                                                                                                                                                                                                                                                  |
| demarc                            | Demarcation point between carrier equipment and CPE.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| designated bridge                 | Bridge that incurs the lowest path cost when forwarding a frame from a segment to the root bridge.                                                                                                                                                                                                                                                                                                                                                                                                  |
| designated router                 | OSPF router that generates link-state advertisements for a multi-access network and has other special responsibilities in running OSPF. Each multi-access OSPF network that has at least two attached routers has a designated router that is elected by the OSPF Hello protocol. The designated router enables a reduction in the number of adjacencies required on a multi-access network, which in turn reduces the amount of routing protocol traffic and the size of the topological database. |
| destination address               | Address of a network device that is receiving data.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| distance vector routing algorithm | Class of routing algorithms that iterate on the number of hops in a route to find a shortest-path spanning tree. Distance vector routing algorithms call for each router to send its entire routing table in each update, but only to its neighbors. Distance vector routing algorithms can be prone to routing loops, but are computationally simpler than link-state routing algorithms. Also called Bellman-Ford routing algorithm.                                                              |

| Acronym or Term         | Definition                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DLCI                    | data-link connection identifier. Value that specifies a PVC or an SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant. (Connected devices might use different values to specify the same connection.) In the LMI extended specification, DLCIs are globally significant (DLCIs specify individual end devices).                                          |
| dot address             | Refers to the common notation for IP addresses in the form <i>n.n.n.n</i> where each number <i>n</i> represents, in decimal, 1 byte of the 4-byte IP address. Also called dotted notation and four-part dotted notation.                                                                                                                                                                                 |
| dotted decimal notation | Syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. Used to represent IP addresses on the Internet, as in 192.67.67.20. Also called dotted quad notation.                                                                                                                                                          |
| dynamic routing         | Routing that adjusts automatically to network topology or traffic changes. Also called adaptive routing.                                                                                                                                                                                                                                                                                                 |
| E1                      | Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.                                                                                                                                                                                                                               |
| encapsulation           | Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data-link layer protocol of the other network.                                                                                       |
| Ethernet                | Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.                                                                                                                            |
| EXEC                    | Interactive command processor of Cisco IOS.                                                                                                                                                                                                                                                                                                                                                              |
| Fast Ethernet           | Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification. |
| FECN                    | forward explicit congestion notification. Bit set by a Frame Relay network to inform the DTE receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow-control action as appropriate.                                                                                     |
| flash memory            | A special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can be updated easily if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.  |
| frame                   | Logical grouping of information sent as a data-link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit.                                                                                                                                                                    |
| Frame Relay             | Industry-standard, switched data-link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it generally is considered a replacement.                                                                                                                                                |
| FRF.5                   | Frame Relay-to-ATM Service Interworking. Allows Frame Relay traffic to be transported through an ATM network.                                                                                                                                                                                                                                                                                            |
| FRF.8                   | Frame Relay-to-ATM Service Interworking. Allows Frame Relay and ATM networks to exchange data despite differing network protocols.                                                                                                                                                                                                                                                                       |
| full duplex             | Capability for simultaneous data transmission between a sending station and a receiving station.                                                                                                                                                                                                                                                                                                         |
| full mesh               | Term describing a network in which devices are organized in a mesh topology, with each network node having either a physical circuit or a virtual circuit connecting it to every other network node. A full mesh provides a great deal of redundancy but because it can be prohibitively expensive to implement, it usually is reserved for network backbones.                                           |

| Acronym or Term         | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| half duplex             | Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| header                  | Control information placed before data when encapsulating that data for network transmission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| hierarchical addressing | Scheme of addressing that uses a logical hierarchy to determine location. For example, IP addresses consist of network numbers, subnet numbers, and host numbers, which IP routing algorithms use to route the packet to the appropriate location.                                                                                                                                                                                                                                                                                                                                                                                                  |
| hierarchical routing    | The complex problem of routing on large networks can be simplified by reducing the size of the networks. This is accomplished by breaking a network into a hierarchy of networks, where each level is responsible for its own routing.                                                                                                                                                                                                                                                                                                                                                                                                              |
| hop                     | Passage of a data packet between two network nodes (for example, between two routers).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| hop count               | Routing metric used to measure the distance between a source and a destination. RIP uses hop count as its sole metric.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| host                    | Computer system on a network. Similar to node, except that host usually implies a computer system, whereas node generally applies to any networked system, including access servers and routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| host name               | Name given to a machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| IEEE 802.1              | IEEE specification that describes an algorithm that prevents bridging loops by creating a spanning tree. The algorithm was invented by Digital Equipment Corporation. The Digital algorithm and the IEEE 802.1 algorithm are not exactly the same, nor are they compatible.                                                                                                                                                                                                                                                                                                                                                                         |
| IEEE 802.3              | IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data-link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet.                                                                                                                                                                                                                                                                                                                                                      |
| internat                | Short for internetwork. Not to be confused with the Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Internet                | Largest global internetwork, connecting tens of thousands of networks worldwide and having a "culture" that focuses on research and standardization based on real-life use. Many leading-edge network technologies come from the Internet community. The Internet evolved in part from ARPANET. At one time, called the DARPA Internet.                                                                                                                                                                                                                                                                                                             |
| internetwork            | Collection of networks interconnected by routers and other devices that functions (generally) as a single network. Sometimes called an internet, which is not to be confused with the Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| internetworking         | General term used to refer to the industry devoted to connecting networks together. The term can refer to products, procedures, and technologies.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IP address              | 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address. |
| ISDN                    | Integrated Services Digital Network. Communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IS-IS                   | Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric to determine network topology.                                                                                                                                                                                                                                                                                                                                                                                                                |
| ISL                     | Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| kbps                    | kilobits per second. A bit rate expressed in thousands of bits per second.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Acronym or Term              | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN                          | local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data-link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.                                                    |
| LAN switch                   | High-speed switch that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches often are categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multilayer switches are an intelligent subset of LAN switches.                                                                  |
| LCP                          | link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.                                                                                                                                                                                                                                                                                                                                                                            |
| learning bridge              | Bridge that performs MAC address learning to reduce traffic on the network. Learning bridges manage a database of MAC addresses and the interfaces associated with each address.                                                                                                                                                                                                                                                                                                         |
| leased line                  | Transmission line reserved by a communications carrier for the private use of a customer. A leased line is a type of dedicated line.                                                                                                                                                                                                                                                                                                                                                     |
| line card                    | Any I/O card that can be inserted in a modular chassis.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| link-state routing algorithm | Routing algorithm in which each router broadcasts or multicasts information regarding the cost of reaching each of its neighbors to all nodes in the internetwork. Link-state algorithms create a consistent view of the network and therefore are not prone to routing loops; however, they achieve this at the cost of relatively greater computational difficulty and more widespread traffic (compared with distance vector routing algorithms).                                     |
| LMI                          | Local Management Interface. Set of enhancements to the basic Frame Relay specification. LMI includes support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which provides the network server with its local DLCI and the multicast DLCI; global addressing, which gives DLCIs global rather than local significance in Frame Relay networks; and a status mechanism, which provides an on-going status report on the DLCIs known to the switch. |
| LSA                          | link-state advertisement. Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.                                                                                                                                                                                                                                                                               |
| MAC                          | Media Access Control. Lower of the two sublayers of the data-link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.                                                                                                                                                                                                                                                                                  |
| MAC address                  | Standardized data-link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, and physical address.                                                                                   |
| MAC address learning         | Service that characterizes a learning bridge, in which the source MAC address of each received packet is stored so that future packets destined for that address can be forwarded only to the bridge interface on which that address is located. Packets destined for unrecognized addresses are forwarded out every bridge interface. This scheme helps minimize traffic on the attached LANs. MAC address learning is defined in the IEEE 802.1 standard.                              |
| NBMA                         | nonbroadcast multi-access. Term describing a multi-access network that either does not support broadcasting (such as X.25) or in which broadcasting is not feasible (for example, an SMDS broadcast group or an extended Ethernet that is too large).                                                                                                                                                                                                                                    |
| Mbps                         | megabits per second. A bit rate expressed in millions of binary bits per second.                                                                                                                                                                                                                                                                                                                                                                                                         |
| modem                        | modulator-demodulator. Device that converts digital and analog signals. At the source, a modem converts digital signals to a form suitable for transmission over analog communication facilities. At the destination, the analog signals are returned to their digital form. Modems allow data to be transmitted over voice-grade telephone lines.                                                                                                                                       |

| Acronym or Term     | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| multilayer switch   | Switch that filters and forwards packets based on MAC addresses and network addresses. A subset of LAN switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Multilink PPP       | Multilink Point-to-Point Protocol. This protocol is a method of splitting, recombining, and sequencing datagrams across multiple logical data links.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| name server         | Server connected to a network that resolves network names into network addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NAT                 | Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.                                                                                                                                                                                                                                                                                                   |
| NCP                 | Network Control Protocol. Series of protocols for establishing and configuring different network layer protocols, such as for AppleTalk over PPP.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| neighboring routers | In OSPF, two routers that have interfaces to a common network. On multi-access networks, neighbors are discovered dynamically by the OSPF Hello protocol.                                                                                                                                                                                                                                                                                                                                                                                                               |
| network address     | Network layer address referring to a logical, rather than a physical, network device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| network management  | Generic term used to describe systems or actions that help maintain, characterize, or troubleshoot a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| NIC                 | network interface card. Board that provides network communication capabilities to and from a computer system. Also called an adapter.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| NVRAM               | nonvolatile RAM. RAM that retains its contents when a unit is powered off.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| OIR                 | online insertion and removal. Feature that permits the addition, the replacement, or the removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown. Sometimes called hot swapping or power-on servicing.                                                                                                                                                                                                                                                                                   |
| OSI reference model | Open System Interconnection reference model. Network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are implemented in hardware and software whereas the upper five layers are implemented only in software. The highest layer (the application layer) is closest to the user. |
| OSPF                | Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.                                                                                                                                                                                                                                                                                       |
| packet              | Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data.                                                                                                                                                                                                                                                                                                                                                                                     |
| packet switching    | Networking method in which nodes share bandwidth with each other by sending packets. Compare with circuit switching and message switching.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PAP                 | Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines.                                       |
| partial mesh        | Network in which devices are organized in a mesh topology with some network nodes organized in a full mesh but others that are connected only to one or two other nodes in the network. A partial mesh does not provide the level of redundancy of a full mesh topology but is less expensive to implement. Partial mesh topologies generally are used in the peripheral networks that connect to a fully meshed backbone.                                                                                                                                              |

| Acronym or Term        | Definition                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PAT                    | port address translation. Translation method that allows the user to conserve addresses in the global address pool by allowing source ports in TCP connections or UDP conversations to be translated. Different local addresses then map to the same global address, with port translation providing the necessary uniqueness.                                                                       |
| ping                   | packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.                                                                                                                                                                                                                                                                     |
| poison reverse updates | Routing updates that explicitly indicate that a network or a subnet is unreachable, rather than implying that a network is unreachable by not including it in updates. Poison reverse updates are sent to defeat large routing loops.                                                                                                                                                                |
| port                   | Interface on an internetworking device (such as a router).                                                                                                                                                                                                                                                                                                                                           |
| PPP                    | Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP. |
| PRI                    | Primary Rate Interface. ISDN interface to primary rate access. Primary rate access consists of a single 64-kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.                                                                                                                                                                                                                      |
| protocol               | Formal description of a set of rules and conventions that govern how devices on a network exchange information.                                                                                                                                                                                                                                                                                      |
| PVC                    | permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.                                                                                                  |
| PVST+                  | per-VLAN spanning tree. Support for Dot1q trunks to map multiple spanning trees to a single spanning tree.                                                                                                                                                                                                                                                                                           |
| RAM                    | random-access memory. Volatile memory that can be read and written by a microprocessor.                                                                                                                                                                                                                                                                                                              |
| rcp                    | remote copy protocol. Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.                                                                                                                                                                                      |
| redundant system       | Computer, router, switch, or other system that contains two or more of each of the most important subsystems, such as two disk drives, two CPUs, or two power supplies.                                                                                                                                                                                                                              |
| reliability            | Total number of system failures, regardless of whether a given failure results in system down time.                                                                                                                                                                                                                                                                                                  |
| remote system          | End system or router that is attached to a remote access network and that is either the initiator or the recipient of a call.                                                                                                                                                                                                                                                                        |
| RFC                    | Request For Comments. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.                                                               |
| RIP                    | Routing Information Protocol. IGP supplied with UNIX BSD systems. The most common IGP in the Internet. RIP uses hop count as a routing metric.                                                                                                                                                                                                                                                       |
| RMON                   | remote monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.                                                                                                                                                          |
| ROM                    | read-only memory. Nonvolatile memory that can be read, but not written, by the microprocessor.                                                                                                                                                                                                                                                                                                       |
| root bridge            | Exchanges topology information with designated bridges in a spanning-tree implementation to notify all other bridges in the network when topology changes are required. This prevents loops and provides a measure of defense against link failure.                                                                                                                                                  |

| Acronym or Term         | Definition                                                                                                                                                                                                                                                                                                                       |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| route                   | Path through an internetwork.                                                                                                                                                                                                                                                                                                    |
| route summarization     | Consolidation of advertised addresses in OSPF and IS-IS. In OSPF, this causes a single summary route to be advertised to other areas by an area border router.                                                                                                                                                                   |
| routed protocol         | Protocol that can be routed by a router. A router must be able to interpret the logical internetwork as specified by that routed protocol. Examples of routed protocols include AppleTalk, DECnet, and IP.                                                                                                                       |
| router                  | Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated). |
| routing                 | Process of finding a path to a destination host. Routing is very complex in large networks because of the many potential intermediate destinations a packet might traverse before reaching its destination host.                                                                                                                 |
| routing domain          | Group of end systems and intermediate systems operating under the same set of administrative rules. Within each routing domain is one or more areas, each uniquely identified by an area address.                                                                                                                                |
| routing metric          | Method by which a routing algorithm determines that one route is better than another. This information is stored in routing tables. Metrics include bandwidth, communication cost, delay, hop count, load, MTU, path cost, and reliability. Sometimes referred to simply as a metric.                                            |
| routing protocol        | Protocol that accomplishes routing through the implementation of a specific routing algorithm. Examples of routing protocols include IGRP, OSPF, and RIP.                                                                                                                                                                        |
| routing table           | Table stored in a router or some other internetworking device that keeps track of routes to particular network destinations and, in some cases, metrics associated with those routes.                                                                                                                                            |
| routing update          | Message sent from a router to indicate network reachability and associated cost information. Routing updates typically are sent at regular intervals and after a change in network topology.                                                                                                                                     |
| segment                 | Section of a network that is bounded by bridges, routers, or switches.                                                                                                                                                                                                                                                           |
| serial transmission     | Method of data transmission in which the bits of a data character are transmitted sequentially over a single channel.                                                                                                                                                                                                            |
| SNMP                    | Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.                                                                        |
| source address          | Address of a network device that is sending data.                                                                                                                                                                                                                                                                                |
| spanning tree           | Loop-free subset of a network topology.                                                                                                                                                                                                                                                                                          |
| spanning-tree algorithm | Algorithm used by the Spanning Tree Protocol to create a spanning tree.                                                                                                                                                                                                                                                          |
| SPF                     | shortest path first algorithm. Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.                                                                                                              |
| split-horizon updates   | Routing technique in which information about routes is prevented from exiting the router interface through which that information was received. Split-horizon updates are useful in preventing routing loops.                                                                                                                    |
| static route            | Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.                                                                                                                                                                           |

| Acronym or Term          | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STP                      | Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version. |
| stub network             | Network that has only a single connection to a router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| subinterface             | One of a number of virtual interfaces on a single physical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| subnet address           | Portion of an IP address that is specified as the subnetwork by the subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| subnet mask              | 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address. Sometimes referred to simply as mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| subnetwork               | In IP networks, a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks.                                                                                                                                                                                                                                                                                                                                                                                                 |
| SVC                      | switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. See also virtual circuit. Called a switched virtual connection in ATM terminology.                                                                                                                                                                                                                                                                                                                                                                                                       |
| switch                   | Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data-link layer of the OSI model.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| switched LAN             | LAN implemented with LAN switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| switching                | Process of taking an incoming frame from one interface and delivering it through another interface. Routers use Layer 3 switching to route a packet, and Layer 2 switches use Layer 2 switching to forward frames.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| synchronous transmission | Term describing digital signals that are transmitted with precise clocking. Such signals have the same frequency, with individual characters encapsulated in control bits (called start bits and stop bits) that designate the beginning and the end of each character.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| T1                       | Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| T3                       | Digital WAN carrier facility. T3 transmits DS-3-formatted data at 44.736 Mbps through the telephone switching network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| TCP/IP                   | Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Telnet                   | Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| terminal                 | Simple device at which data can be entered or retrieved from a network. Generally, terminals have a monitor and a keyboard, but no processor or local disk drive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| terminal emulation       | Network application in which a computer runs software that makes it appear to a remote host as a directly attached terminal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| terminal server          | Communications processor that connects asynchronous devices, such as terminals, printers, hosts, and modems, to any LAN or WAN that uses TCP/IP, X.25, or LAT protocols. Terminal servers provide the internetwork intelligence that is not available in the connected devices.                                                                                                                                                                                                                                                                                                                                                                                                               |
| TFTP                     | Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Acronym or Term | Definition                                                                                                                                                                                                                                                                                                                                      |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| throughput      | Rate of information arriving at, and possibly passing through, a particular point in a network system.                                                                                                                                                                                                                                          |
| topology        | Physical arrangement of network nodes and media within an enterprise networking structure.                                                                                                                                                                                                                                                      |
| traceroute      | Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.                                                                                                                                           |
| trunk           | Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.                                                                                                                                                                                                        |
| tunnel          | Secure communication path between two peers, such as two routers.                                                                                                                                                                                                                                                                               |
| tunneling       | Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.                                                                                                                                                                                                                  |
| virtual circuit | Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC.                  |
| VLAN            | virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. |
| VLSM            | variable length subnet mask. Capability to specify a different subnet mask for the same network number on different subnets. VLSM can help optimize available address space.                                                                                                                                                                    |
| vty             | virtual type terminal. Virtual type terminal commonly used as virtual terminal lines.                                                                                                                                                                                                                                                           |
| WAN             | wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.                                                                                                                              |
| WIC             | WAN interface card. Connects the system to the WAN link service provider.                                                                                                                                                                                                                                                                       |
| wildcard mask   | A 32-bit quantity used in conjunction with an IP address to determine which bits in an IP address should be ignored when comparing that address with another IP address. A wildcard mask is specified when setting up access lists.                                                                                                             |

# Lab Guide

---

## Overview

Use the exercises here to complete the lab exercises for this course. The solutions information is found in the Lab Exercise Answer Key.

## Outline

This Lab Guide includes these exercises:

- Lab Exercise 1-1: Cisco Remote Lab Connection
- Lab Exercise 1-2: Configuring the Switch
  - Catalyst 1900 Series Switch Lab Exercise Instructions
  - Catalyst 2950 Series Switch Lab Exercise Instructions
- Lab Exercise 2-1: Configuring a Switch for Extended Functionality
  - Catalyst 1900 Series Switch Lab Exercise Instructions
  - Catalyst 2950 Series Switch Lab Exercise Instructions
- Lab Exercise 3-1: Determining IP Routes with RIP
- Lab Exercise 3-2: Determining IP Routes with IGRP
- Lab Exercise 3-3: Determining IP Routes with EIGRP
- Lab Exercise 3-4: Determining IP Routes with OSPF
- Lab Exercise 4-1: Configuring IP Access Lists
- Lab Exercise 4-2: Configuring Port Address Translation
- Lab Exercise 5-1: Configuring Serial Connections to WAN Service Providers
- Lab Exercise 6-1: Connecting to Frame Relay Services
- Lab Exercise 7-1: Completing an ISDN BRI Call and Configuring DDR

# Laboratory Exercise 1-1: Cisco Remote Lab Connection

Complete the laboratory exercise to practice what you learned in this module.

## Exercise Objective

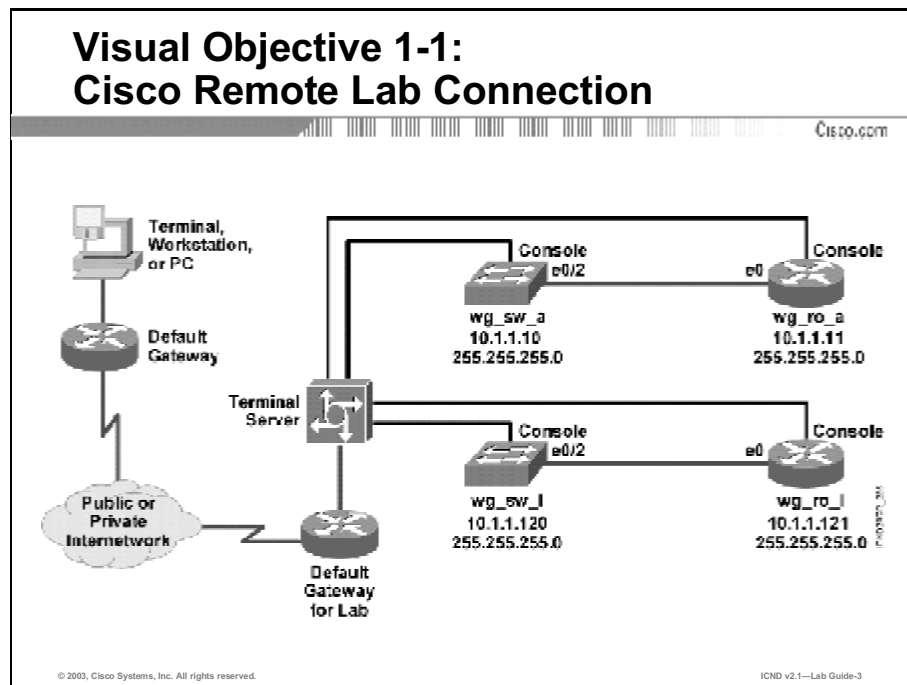
The Cisco router for your pod has all of the cables preconnected and ready for use. Your task in this laboratory exercise is to Telnet to the terminal server to access the devices in your pod.

After completing this exercise, you will be able to:

- Run Telnet to connect to the ICND remote lab
- Verify connectivity to the ICND remote lab terminal server

## Visual Objective

The figure shows the topology that you will work with in this laboratory exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite laboratory, or PC with an Internet connection to access the remote laboratory
- Terminal server connected to a console port of each laboratory device, if using a remote laboratory
- ICND pod assigned by your instructor



## Command List

In this laboratory exercise, you will use the command listed in the table. Refer to this table if you need configuration command assistance during the laboratory exercise.

| Command                        | Description                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <code>telnet ip-address</code> | Starts a terminal emulation program from a PC, router, or switch that permits you to access network devices remotely over the network. |

## Job Aids

There are no job aids for this laboratory exercise.

## Exercise Preparation

Your instructor will provide setup information that you need to complete this and the subsequent laboratory exercises. Your instructor will also assign you to a pod, identified by the letters A through L. Complete the following information as provided by your instructor.

| Value                                  | Information Provided by Your Instructor |
|----------------------------------------|-----------------------------------------|
| Your workgroup                         |                                         |
| IP address of your terminal            |                                         |
| Subnet mask                            |                                         |
| IP address of the default gateway      |                                         |
| IP address of the terminal server      |                                         |
| Username to access the terminal server |                                         |
| Password to access the terminal server |                                         |
| IP address of the TFTP server          |                                         |

## Task 1: Run Telnet to Connect to the ICND Remote Lab

To begin the laboratory exercises, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

### Exercise Procedure

Complete these steps from your PC:

**Step 1** From the Microsoft Windows Start menu, choose **Run**. The Run window appears.

**Step 2** In the Open: field, type the **telnet** command followed by the IP address for your terminal server, provided by your instructor. For example, if the terminal server address that your instructor provided is 10.1.1.254, you would type:

**telnet 10.1.1.254**

If your Telnet session successfully connects to the terminal server, you should see an opening menu similar to the following:

```


 CISCO ICND STUDENT MENU
 CONNECT TO YOUR POD LETTER

ITEM# DEVICE NAME

1 Connect to pod A
2 Connect to pod B
3 Connect to pod C
4 Connect to pod D
5 Connect to pod E
6 Connect to pod F
7 Connect to pod G
8 Connect to pod H
9 Connect to pod I
10 Connect to pod J
11 Connect to pod K
12 Connect to pod L
13 EXIT
```

Please enter selection:

**Step 3** At the "Please enter selection:" prompt, enter your workgroup number and press **Return**. Your output should look similar to the following:

```


 POD L
 To exit back out to the menu press "CTRL+SHIFT+6" then "X".
 You must clear the line before re-connecting to a device.

1 Connect to workgroup switch L
2 Connect to workgroup router L
3 Clear connection to w/g switch L
4 Clear connection to w/g router L
5 Return to main menu
Please enter selection:
```

The menu, called the Pod menu, lists your pod letter at the top. In the example, the current pod is Pod L.

From the menu, you can connect to either your workgroup switch or your workgroup router. Once you connect to a network device from the terminal server, you will need to use a special keystroke sequence, **Ctrl-Shift-6**, then **x**, to return to the menu. (To do this, hold down the **Shift** key, press the **Ctrl** key and the **6**, then press the **x** key.)

**Step 4** Enter **1** to connect to your workgroup switch. You should see the following (or something similar) in your Telnet session:

```
Please enter selection: 1
Trying h26 (10.10.10.10, 2058) ... Open
```

**Step 5** Press **Return** to access the device prompt.

---

**Note** Your output will vary depending on the switch type to which you are connected. On an unconfigured Catalyst 1900 series switch, a menu appears. On an unconfigured Catalyst 2950 series switch, setup mode appears.

---

**Step 6** To return to the menu, enter **Ctrl-Shift-6**, then **x**. The Pod menu appears again.

When you return to the Pod menu, your session to your workgroup switch is still open. You should clear all open connections on a terminal server before exiting. If you do not close your open sessions, the Cisco IOS software will prompt you to close your open connections. To close a session, you must select the appropriate option from the menu.

**Step 7** Enter option **3** to clear the connection to your workgroup switch. When the "[confirm]" prompt appears, press **Return**.

What does the prompt say now?

---

**Step 8** Enter option **2** to connect to your workgroup router.

What does the prompt say now? As with the switch, you may need to press **Return** one time to see the prompt on your terminal screen.

---

**Step 9** Enter **Ctrl-Shift-6**, then **x**, to return to the Pod menu.

**Step 10** Enter option **4** to clear the connection to your workgroup router. When the "[confirm]" prompt appears, press **Return**.

**Step 11** Enter option **5** to return to the Main menu from the Pod menu.

**Step 12** Exit the terminal server by entering the option from the Pod menu to exit. If there is no option to exit on the menu, contact your instructor for instructions.

**Step 13** If you see the "You have open connections [confirm]" prompt, enter **yes** and press **Return**.  
Depending on which operating system is running on your PC, you may need to press **Return** after terminating your Telnet session.

**Step 14** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You can successfully log onto the terminal server and navigate the menus to access your workgroup switch and workgroup router.
- You can clear the connections to your workgroup switch and workgroup router.

# Lab Exercise 1-2: Configuring the Switch

Complete the lab exercise to practice what you learned in this module.

---

**Note** This lab exercise includes two sets of instructions: one for the Catalyst 1900 series and one for the Catalyst 2950 series. Complete only the steps for your model of workgroup switch.

---

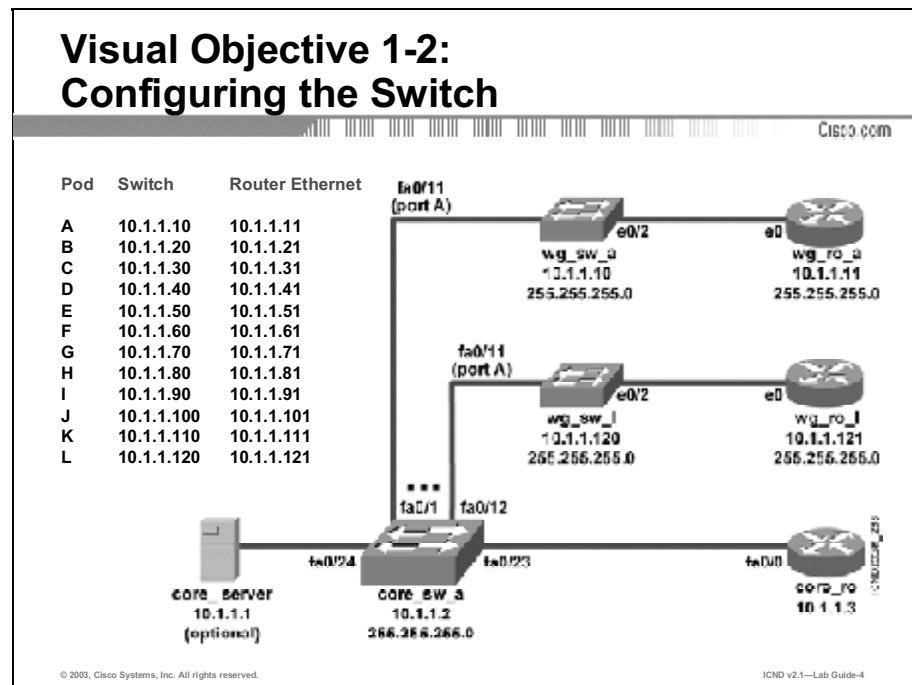
## Exercise Objective

Given a Catalyst 1900 series workgroup switch or a Catalyst 2950 series workgroup switch, you will configure the switch and use the **show** commands to verify your configuration. After completing this exercise, you will be able to meet these objectives:

- Manage the Catalyst switch features
- Configure port security on the Catalyst switch
- Manage the Catalyst switch MAC address table

## Visual Objective

The figure shows the switch configuration that is in this lab exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

In this lab exercise, you will configure a Catalyst switch. Using basic management commands and port security, you will examine the general configuration of the switch and manage the MAC address table. To successfully complete this exercise, your equipment must be properly connected. If you are using remote lab equipment, the connections should be set. If you have a lab onsite, you will need to insure that your equipment is cabled as shown in the Visual Objective for this lab exercise.

Additionally, you need both Ethernet and IP connectivity from the workgroup switch to the core switch, and from the workgroup switch to the workgroup router. The workgroup router is used as a network device when configuring port security, so it is important to verify the IP path from the workgroup switch to the workgroup router. To verify this path, use the **ping** command from the workgroup switch to ping the workgroup router. Ping from the workgroup switch to the TFTP server (10.1.1.1), if one is available. If you are unable to reach either of these devices, ask your instructor for assistance.

The table lists additional parameters that you will need to complete this lab exercise.

| Network Device             | Device Address |
|----------------------------|----------------|
| TFTP server (if available) | 10.1.1.1       |
| Core Switch A              | 10.1.1.2       |
| Core Router                | 10.1.1.3       |

# Catalyst 1900 Series Switch Lab Exercise Instructions

Good network management procedures require that you maintain past configurations as well as Cisco IOS images. TFTP is frequently used to transfer these files over the network and is used in this exercise to copy your configuration to the TFTP server, if one is available. You will also configure security on a port to demonstrate that a MAC address can be “locked” to a physical switch port. Finally, you will statically enter MAC addresses into the switch MAC address table (MAT).

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                                               | Description                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>address-violation disable</code>                                | Disables the port on an address violation when using port security.                                                                                                                                                                                                     |
| <code>copy nvram tftp://10.1.1.1/config.cfg</code>                    | Copies a configuration file from NVRAM to the TFTP server at IP address 10.1.1.1.                                                                                                                                                                                       |
| <code>enable</code>                                                   | Activates the privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.                                                                                   |
| <code>interface type</code>                                           | Specifies an interface or subinterface, and puts the device in interface configuration mode.                                                                                                                                                                            |
| <code>mac-address</code>                                              | Changes the router BIA <sup>1</sup> on an interface.                                                                                                                                                                                                                    |
| <code>mac-address-table permanent mac-address type module/port</code> | Sets a permanent MAC address on the Catalyst 1900 series.                                                                                                                                                                                                               |
| <code>no port secure</code>                                           | Disables port security.                                                                                                                                                                                                                                                 |
| <code>ping ip-address</code>                                          | Common tool used to troubleshoot the accessibility of devices. It uses ICMP <sup>2</sup> echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>port secure max-mac-count count</code>                          | Sets port security.                                                                                                                                                                                                                                                     |
| <code>show interfaces</code>                                          | Displays interface information.                                                                                                                                                                                                                                         |
| <code>show ip</code>                                                  | Displays the switch IP address information.                                                                                                                                                                                                                             |
| <code>show mac-address-table {security}</code>                        | Displays the MAC address table.                                                                                                                                                                                                                                         |
| <code>show version</code>                                             | Displays the configuration of the switch hardware and the various software versions.                                                                                                                                                                                    |
| <code>shutdown/no shutdown</code>                                     | Disables or enables an interface.                                                                                                                                                                                                                                       |

<sup>1</sup> BIA = burned-in address

<sup>2</sup> ICMP = Internet Control Message Protocol

## Task 1: Manage Catalyst 1900 Series Switch Features

In this task, you will copy your switch configuration to the TFTP server (if one is available), to provide a backup copy if you need to restore your switch to a previous state.

Complete the following steps to manage switch features on a Catalyst 1900 series workgroup switch:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup switch from the Pod menu.
- Step 4** Enter privileged EXEC mode using the **enable** command.
- Step 5** Enter the command to display the current configuration of the switch.

Which command is used to copy the startup-config in NVRAM to the TFTP server? Assume that the TFTP server address is 10.1.1.1. Use the filename **wgsw.x.cfg**, where **x** identifies your pod.

---

- Step 6** If your class is using a TFTP server, enter the command to copy the configuration in NVRAM to the TFTP server.

- Step 7** Enter the command to show the Cisco IOS version running at the switch. Check the output to answer the following question:

Which Cisco IOS version is running on the switch?

---

- Step 8** From the EXEC mode, enter the command to show the IP address configuration on the switch.

- Step 9** From the EXEC mode, enter the command to show the MAC address table of the switch.

How many dynamic MAC addresses have been learned?

---

What is the MAC address of the router connected to your switch at port E0/2?

---

- Step 10** Proceed to Task 2.



## Task 2: Configure Port Security on a Switch

In this section, you will configure the switch to permit only a single MAC address on the second access port. After you verify the configuration, you will configure the MAC address on the router to a new address. This address will not be permitted access because you configured port security to deny access. After you verify that the port security has blocked the new MAC address of the router, you will remove that MAC address from the router, and enter the **shutdown/no shutdown** commands on the physical access port to clear the security. At this point, you should be able to ping from router to switch again.

Complete the following steps to configure port security on your workgroup switch:

- Step 1** Enter the global configuration mode.
- Step 2** Enter the **interface ethernet 0/2** command.
- Step 3** Configure the switch to set port e0/2 to secured mode using the **port secure** command.
- Step 4** Enter the command to set the maximum count to 1.
- Step 5** Exit interface configuration mode.
- Step 6** Configure the switch to set the port security violation action for port e0/2 to disable.
- Step 7** Exit global configuration mode.
- Step 8** From the EXEC mode, enter the command to show the current running configurations to verify the port security configuration.

Do you see a permanent MAC address for port e0/2?

---

- Step 9** Enter the command to show the MAC address table from the EXEC mode.

Do you see the router MAC address at port e0/2?

---

What is the router MAC address?

---

- Step 10** Access your **wg\_ro\_x** console port, where **x** identifies your pod.
- Step 11** Ping **wg\_sw\_x**, where **x** identifies your pod letter, to test connectivity to the switch.
- Step 12** Use the command **mac-address 0008.eeee.eeee** interface configuration command to change the MAC address of the first Ethernet interface on the router.
- Step 13** Ping **wg\_sw\_x**, where **x** identifies your pod letter, to verify that you no longer have connectivity to the workgroup switch because of the MAC address change.
- Step 14** Access your **wg\_sw\_x** console port, where **x** identifies your pod.

**Step 15** Enter the **show interface e0/2** command.

What is the status of your e0/2 interface on your **wg\_sw\_x** console now? Why does the switch have this status?

---

**Step 16** Enter the **show running-config** command. You should see a **port-secure** command in the running-config.

**Step 17** Access your **wg\_ro\_x** console port, where **x** identifies your pod.

**Step 18** Use the **no mac-address** interface configuration command to reset the MAC address of the first Ethernet interface on your router, back to the burned-in address (BIA).

**Step 19** Return to privileged EXEC mode.

**Step 20** Access your **wg\_sw\_x** console port, where **x** identifies your pod.

**Step 21** Enter the **no shutdown** command on the e0/2 port on your **wg\_sw\_x** console.

**Step 22** Use the **no port secure** and **port secure max address 132** commands to return the interface to the default values.

**Step 23** Enter the **show interface e0/2** command on your **wg\_sw\_x** console to verify that the interface is back up.

**Step 24** Access your **wg\_ro\_x** console port, where **x** identifies your pod.

**Step 25** Ping **wg\_sw\_x**, where **x** identifies your pod letter, to verify that you have connectivity to the switch again.

**Step 26** Proceed to Task 3.

### Task 3: Manage the MAC Address Table

One feature that you can use to provide security or rapid switching is to make static entries in the MAC address table. You saw in the last task that you can manually assign the MAC address to a router interface. If you need to move equipment, this allows you to leave the configuration of your switch static when you install a new router and hence a new MAC address. Static MAC table entries are populated after power-on self test (POST), eliminating the need for an incoming frame for the switch to learn the address of the device that is associated with a specific switch port. In this section, you will configure a permanent address in your MAC address table.

Complete the following steps to manage the MAC address table on your workgroup switch:

**Step 1** Enter the global configuration mode.

**Step 2** Enter the command to assign a permanent MAC address of AAAA.AAAA.AAAA to port e0/4.

**Step 3** Exit back to the privileged EXEC mode.

**Step 4** Enter the command to show the MAC address table at the EXEC command mode.

Do you see the permanent MAC address you assigned to port e0/4?

---

**Step 5** Return to global configuration mode.

- Step 6** Enter the command to remove the permanent MAC address you entered.
- Step 7** Exit global configuration mode.
- Step 8** From the EXEC mode, enter the command to show the MAC address table to verify the deletion of the permanent MAC address.
- Step 9** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You successfully transfer your startup-config in NVRAM to a TFTP server (optional).
- You observe the IP addressing characteristics of your switch and display the MAC address table.
- You successfully configure port security to permit a single MAC address on a port, then change the MAC address of the device that is connected to that port, thereby disabling the port, and then remove port security and change the MAC address back so that the traffic between the two devices flows normally.
- You successfully configure a static MAC address entry in your workgroup switch.

# Catalyst 2950 Series Switch Lab Exercise Instructions

Good network management procedures require that you maintain past configurations as well as Cisco IOS images. TFTP is frequently used to transfer these files over the network and is used in this exercise to copy your configuration to the TFTP server, if one is available. You will also configure security on a port to demonstrate that a MAC address can be “locked” to a physical switch port. Finally, you will statically enter MAC addresses into the switch MAC address table (MAT).

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                                                          | Description                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clear arp-cache</code>                                                     | Clears the IP ARP <sup>1</sup> cache.                                                                                                                                                                                                                                |
| <code>copy startup-config tftp</code>                                            | Copies the startup configuration file to a TFTP server.                                                                                                                                                                                                              |
| <code>enable</code>                                                              | Activates the privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.                                                                                |
| <code>mac-address</code>                                                         | Changes the router BIA on an interface.                                                                                                                                                                                                                              |
| <code>mac-address-table static mac-address interface interface vlan vlan#</code> | Sets a permanent MAC address on the Catalyst 2950 series.                                                                                                                                                                                                            |
| <code>no mac-address-table secure mac-address vlan 1</code>                      | Enters the secure MAC address, its associated port, and VLAN ID to be removed.                                                                                                                                                                                       |
| <code>ping ip-address</code>                                                     | Common tool used to troubleshoot the accessibility of devices. It uses ICMP Path Echo requests and ICMP Path Echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>port secure [max-mac-count count]</code>                                   | Sets port security.                                                                                                                                                                                                                                                  |
| <code>port security action shutdown</code>                                       | Sets the port to shutdown when a security violation occurs.                                                                                                                                                                                                          |
| <code>show interfaces</code>                                                     | Displays interface information.                                                                                                                                                                                                                                      |
| <code>show mac-address-table {secure}</code>                                     | Displays the MAC address table.                                                                                                                                                                                                                                      |
| <code>show running-config</code>                                                 | Displays the active configuration.                                                                                                                                                                                                                                   |
| <code>show version</code>                                                        | Displays the configuration of the switch hardware and the various software versions.                                                                                                                                                                                 |
| <code>shutdown/no shutdown</code>                                                | Disables or enables an interface.                                                                                                                                                                                                                                    |

<sup>1</sup> ARP = Address Resolution Protocol

## Task 1: Manage Catalyst 2950 Series Switch Features

In this task, you will copy your switch configuration to the TFTP server, if one is available, in order to provide a backup copy if you need to restore your switch to a previous state.

Complete the following steps to manage switch features on a Catalyst 2950 series workgroup switch:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select the workgroup switch from the Pod menu.
- Step 4** Use the **enable** command to enter privileged EXEC mode.
- Step 5** Enter the command to display the startup-config of the switch.

Which command is used to copy the startup-config in NVRAM to the TFTP server? Assume that the TFTP server address is 10.1.1.1. Use the filename **wgswx.cfg**, where **x** identifies your pod.

---

- Step 6** If your class is using a TFTP server, enter the command to copy the startup-config in NVRAM to the TFTP server.

- Step 7** Enter the command to show the Cisco IOS version running at the switch and check the output to answer the following question:

Which Cisco IOS version is running on the switch?

---

- Step 8** From the EXEC mode, enter the command to show the IP address configuration that is on the switch.

- Step 9** From the EXEC mode, enter the command to show the MAC address table of the switch.

How many dynamic MAC addresses have been learned?

---

What is the MAC address of the router that is connected to your switch at port fa 0/2?

---

- Step 10** Proceed to Task 2.

## Task 2: Configure Port Security on a Switch

In this task, you will configure the switch to permit only a single MAC address on the second access port. After you verify the configuration, you will configure the MAC address on the router to a new address. This address will not be permitted access because you configured port security to deny access. After you verify that the port security has blocked the new MAC address of the router, you will remove that MAC address from the router, and enter the **shutdown/no shutdown** commands on the physical access port to clear the security. At this point you should be able to ping from router to switch again.

Complete the following steps to configure port security on the workgroup switch:

- Step 1** Enter the command to set port fa 0/2 to secured mode with a max-mac-count of 1.
- Step 2** Enter the command to set the port security violation action for port fa 0/2 to shutdown.
- Step 3** Enter the command to show the current running configuration in order to verify the port security configuration.

Do you see a secure MAC address on port fa 0/2?

---

- Step 4** Enter the command to show the secure mac-address-table.

Do you see your router MAC address at port fa0/2? What is the router MAC address?

---

- Step 5** Access your **wg\_ro\_x** console port, where **x** identifies your pod.
- Step 6** Use the **mac-address 0008.eeee.eeee** interface configuration command to change the MAC address of the first Ethernet interface on your router.
- Step 7** Exit the global configuration mode.
- Step 8** Access your **wg\_sw\_x** console port, where **x** identifies your pod.
- Step 9** Enter the **show interface fa 0/2** command.

What is the status of your fa 0/2 interface on your **wg\_sw\_x** console now? Why does the switch have this status?

---

- Step 10** Enter the **show running-config** command. You should see a **mac-address table secure** command in the running-config.
- Step 11** Access your **wg\_ro\_x** console port, where **x** identifies your pod letter.
- Step 12** Use the **no mac** interface configuration command to reset the MAC address of the first Ethernet interface on your router, back to the burned-in address (BIA).
- Step 13** Exit the global configuration mode.
- Step 14** Access your **wg\_sw\_x** console port, where **x** identifies your pod.
- Step 15** Use the **no mac-address-table secure mac-address vlan 1** command to remove the secured MAC address.

- Step 16** Enter the **no shutdown** command on the fa 0/2 port on your **wg\_sw\_x** console.
- Step 17** Enter the **show interface fa 0/2** command on your **wg\_sw\_x** console to verify the interface is back up.
- Step 18** Clear the ARP cache on your workgroup switch using the **clear arp-cache** command.
- Step 19** Ping your workgroup router to test connectivity.
- Step 20** Proceed to Task 3.

### Task 3: Manage the MAC Address Table

One feature that provides security or rapid switching is to make static entries in the MAC address table. You can manually assign the MAC address to a router interface. If you need to move equipment, this feature permits you to leave the configuration of your switch static when you install a new router and hence a new MAC address. Static MAC table entries are populated after power-on self test (POST), eliminating the need for an incoming frame for the switch to learn the address of the device associated with a specific switch port. In this task, you will configure a permanent address in your MAC address table.

Complete the following steps to manage the MAC address table on your workgroup switch:

- Step 1** In global configuration mode, enter the command to assign a permanent MAC address of AAAA.AAAA.AAAA to port fa 0/4 in VLAN 1. Exit global configuration mode when completed.
- Step 2** From the EXEC mode, enter the command to show the MAC address table.
- Do you see the permanent MAC address you assigned to port fa0/4?
- 
- Step 3** In global configuration mode, enter the command to remove the permanent MAC address you entered.
- Step 4** Exit the global configuration mode.
- Step 5** From the EXEC mode, enter the command to show the MAC address table in order to verify the deletion of the permanent MAC address. Make sure that all the permanent addresses configured are removed.
- Step 6** Enter the **show run** command to determine if you have a secure MAC address on your fa 0/2 interface.
- Step 7** Remove the secure MAC address on your fa 0/2 interface, if one exists, using the **no mac-address-table secure** command.
- Step 8** Disable port security on your fa 0/2 interface.
- Step 9** Notify your instructor that you have completed the exercise.

### Exercise Verification

You have completed this exercise when you attain these results:

- You limited port fa 0/2 on your workgroup switch to a single MAC address usage.
- You assigned and removed a permanent MAC address to port fa 0/4.

# Lab Exercise 2-1: Configuring a Switch for Extended Functionality

Complete the lab exercise to practice what you learned in this module.

---

**Note** This lab exercise includes two sets of instructions: one for the Catalyst 1900 series and one for the Catalyst 2950 series. Complete only the steps for your model of workgroup switch.

---

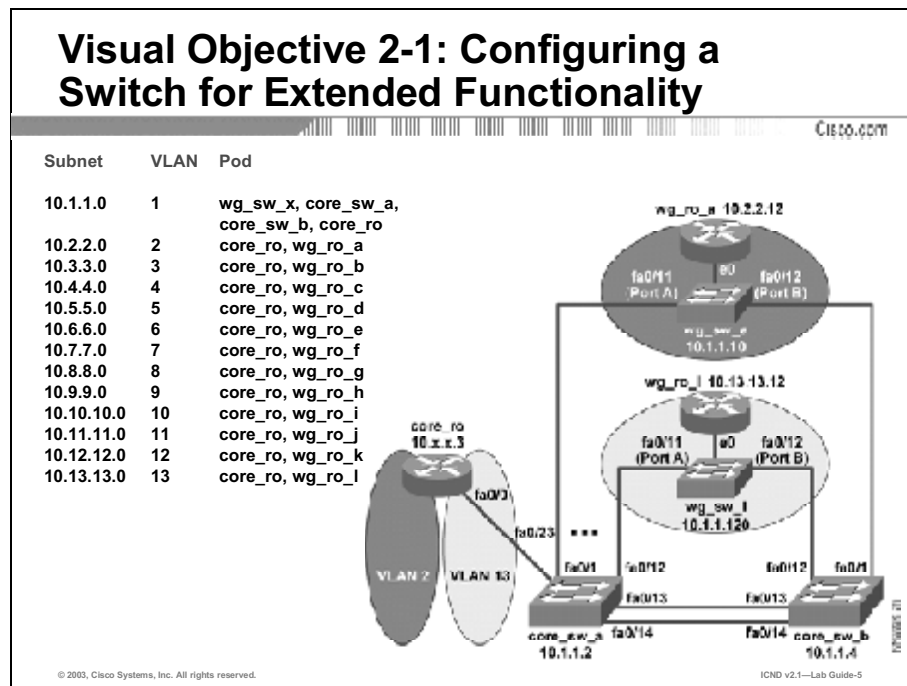
## Exercise Objective

Given a switch and VLAN requirements, you will configure a switch to meet the stated requirements. Specifically, you will configure the VLAN Trunking Protocol (VTP) and the VTP mode, add another VLAN to your workgroup switch, configure trunking, and be able to describe the tools that are used to monitor the Spanning Tree Protocol (STP) in operation on a switch. After completing this exercise, you will be able to meet these objectives:

- Configure VTP and a VTP domain on a switch
- Assign a switch to the appropriate VTP mode to meet its operational requirements
- Configure separate VLANs on a Catalyst switch
- Configure and monitor the STP

## Visual Objective

The figure shows the configuration that you will complete in this lab exercise.





## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

To prepare for this lab exercise, complete the following steps:

- Verify that you have a single connection between the workgroup switch and core switch A by using the **show cdp neighbors** command. Verify that the only core neighbor you see is core\_sw\_a.
- Your instructor needs to load new configurations on the core switches. Check with the instructor to be certain this has been completed.

## Catalyst 1900 Series Fast Ethernet Connections

On the Catalyst 1900 series, use the following table, which lists the Fast Ethernet connections that are necessary to complete this lab exercise.

| Pod Name | Pod Port | Core A Port | Pod Port | Core B Port |
|----------|----------|-------------|----------|-------------|
| Pod A    | fa0/26   | fa0/1       | fa0/27   | fa0/1       |
| Pod B    | fa0/26   | fa0/2       | fa0/27   | fa0/2       |
| Pod C    | fa0/26   | fa0/3       | fa0/27   | fa0/3       |
| Pod D    | fa0/26   | fa0/4       | fa0/27   | fa0/4       |
| Pod E    | fa0/26   | fa0/5       | fa0/27   | fa0/5       |
| Pod F    | fa0/26   | fa0/6       | fa0/27   | fa0/6       |
| Pod G    | fa0/26   | fa0/7       | fa0/27   | fa0/7       |
| Pod H    | fa0/26   | fa0/8       | fa0/27   | fa0/8       |
| Pod I    | fa0/26   | fa0/9       | fa0/27   | fa0/9       |
| Pod J    | fa0/26   | fa0/10      | fa0/27   | fa0/10      |
| Pod K    | fa0/26   | fa0/11      | fa0/27   | fa0/11      |
| Pod L    | fa0/26   | fa0/12      | fa0/27   | fa0/12      |

## Catalyst 2950 Series Fast Ethernet Connections

On the Catalyst 2950 series, use the following table, which lists the Fast Ethernet connections that are necessary to complete this lab exercise.

| Pod Name | Pod Port | Core A Port | Pod Port | Core B Port |
|----------|----------|-------------|----------|-------------|
| Pod A    | fa0/11   | fa0/1       | fa0/12   | fa0/1       |
| Pod B    | fa0/11   | fa0/2       | fa0/12   | fa0/2       |
| Pod C    | fa0/11   | fa0/3       | fa0/12   | fa0/3       |
| Pod D    | fa0/11   | fa0/4       | fa0/12   | fa0/4       |
| Pod E    | fa0/11   | fa0/5       | fa0/12   | fa0/5       |
| Pod F    | fa0/11   | fa0/6       | fa0/12   | fa0/6       |
| Pod G    | fa0/11   | fa0/7       | fa0/12   | fa0/7       |
| Pod H    | fa0/11   | fa0/8       | fa0/12   | fa0/8       |
| Pod I    | fa0/11   | fa0/9       | fa0/12   | fa0/9       |
| Pod J    | fa0/11   | fa0/10      | fa0/12   | fa0/10      |
| Pod K    | fa0/11   | fa0/11      | fa0/12   | fa0/11      |
| Pod L    | fa0/11   | fa0/12      | fa0/12   | fa0/12      |

## Catalyst 1900 Series Switch Lab Exercise Instructions

In this exercise, you will configure your workgroup switch to participate in a VTP domain in the transparent mode. This will prevent VLAN changes made on the workgroup switch from propagating to other switches in the lab.

Your instructor has configured the core switches to trunk to the workgroup switches from their previous nontrunking mode. This effectively prevents frames from passing between the core switches and the workgroup switches, and blocks your access to the core devices.

You will configure trunking on one of the trunk ports so that you can reach the core router again. You will also configure a VLAN for the switch port that is connected to your workgroup router and change the IP address of the first Ethernet interface on your workgroup router. The new address is one that is in the VLAN assigned to your pod and can only reach other devices in the workgroup (in a different VLAN) via the core router.

Your instructor has configured the core router to support interVLAN routing. Finally, you will configure the second trunk port on your workgroup switch for trunking to core\_sw\_b and observe the STP convergence when a loop is built.

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                                                                   | Description                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>                                                                             | Activates the privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.                                                                              |
| <b>interface</b> <i>interface</i><br><b>trunk on</b>                                      | Configures a Fast Ethernet interface to be in Inter-Switch Link (ISL) trunking mode.                                                                                                                                                                               |
| <b>interface</b> <i>interface</i><br><b>vlan-membership</b><br><b>static</b> <i>vlan#</i> | Assigns a port to a VLAN.                                                                                                                                                                                                                                          |
| <b>ip address</b> <i>ip-address</i><br><i>mask</i>                                        | Defines the IP address and subnet mask for the selected interface.                                                                                                                                                                                                 |
| <b>ip route</b> <b>network</b> <i>mask</i><br><i>next-hop-router-</i><br><i>address</i>   | Establishes static routes.                                                                                                                                                                                                                                         |
| <b>ping</b> <CR>                                                                          | If an extended <b>ping</b> command is used, you will set the ping count manually. (Use this command in privileged EXEC mode.)                                                                                                                                      |
| <b>ping</b> <i>ip-address</i>                                                             | Common tool that is used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <b>show cdp neighbors</b>                                                                 | Displays detailed information about neighboring devices discovered using CDP <sup>1</sup> .                                                                                                                                                                        |
| <b>show interface</b><br><i>interface</i>                                                 | Displays the trunk parameters.                                                                                                                                                                                                                                     |
| <b>show ip interface</b><br><i>type</i>                                                   | Lists a summary of an interface IP information and status.                                                                                                                                                                                                         |
| <b>show spantree</b> <i>vlan#</i>                                                         | Displays spanning-tree information for a particular VLAN.                                                                                                                                                                                                          |
| <b>show trunk</b>                                                                         | Displays trunk parameters.                                                                                                                                                                                                                                         |
| <b>show vlan</b>                                                                          | Displays information on all configured VLANs.                                                                                                                                                                                                                      |
| <b>show vtp</b>                                                                           | Displays VTP information.                                                                                                                                                                                                                                          |
| <b>shutdown/no shutdown</b>                                                               | Disables or enables an interface.                                                                                                                                                                                                                                  |
| <b>vlan</b> <i>vlan#</i> <b>name</b> <i>vlan-</i><br><i>name</i>                          | Defines a VLAN and VLAN name.                                                                                                                                                                                                                                      |
| <b>vtp transparent</b>                                                                    | Specifies the operating mode, domain name, password, generation of traps, and pruning capabilities of VTP.                                                                                                                                                         |
| <b>vtp domain</b> <i>domain</i>                                                           | Sets the VTP administrative domain.                                                                                                                                                                                                                                |

<sup>1</sup> CDP = Cisco Discovery Protocol

## Task 1: Configure VTP and VTP Domains

In this exercise, you will configure your workgroup switch to participate in a VTP domain in the transparent mode. This will prevent VLAN changes made on the workgroup switch from propagating to other switches in the lab.

Complete the following steps on your workgroup switch:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup switch from the Pod menu.
- Step 4** Enter privileged EXEC mode using the **enable** command.
- Step 5** Set the VTP domain name to “ICND” and the mode to transparent.

What command sequence do you use to set the domain name and VTP mode on your workgroup switch?

- 
- Step 6** Verify the VTP configuration using the **show vtp** command.

Is the domain name the same that you entered? Are you in transparent mode?

- 
- Step 7** Proceed to Task 2.

## Task 2: Assign a Switch to the Appropriate VTP Mode

The instructor has configured the core switches to trunk to the workgroup switches from their previous nontrunking mode. This effectively shuts off frames from passing between the core switches and the workgroup switches and blocks your access to the core devices. You will configure trunking on one of the trunk ports so that you can reach the core router again.

Complete the following steps to configure trunking mode on your workgroup switch:

- Step 1** Set the port fa0/26 at your workgroup switch to trunk mode.

What command do you use to set the port to trunk mode?

- 
- Step 2** Verify the trunk configuration.

What command do you use to display a trunk configuration?

- 
- Step 3** To verify trunking, **ping** the router at 10.1.1.3 from the workgroup switch. (If it does not work, wait a few minutes and try again.)
  - Step 4** Proceed to Task 3.

### Task 3: Configure Separate VLANs on the Switch

In this task, you will configure a VLAN for the switch port that is connected to your workgroup router and change the IP address of the first Ethernet interface on your workgroup router. The new address is one that is in the VLAN assigned to your pod and can only reach other devices in the workgroup (in a different VLAN) via the core router. Your instructor has configured the core router to support interVLAN routing.

The table, or VLAN assignment chart, provides information you need to complete this task.

| Pod | VLAN Number | VLAN Name | core_ro_x<br>(where x is your pod letter) |
|-----|-------------|-----------|-------------------------------------------|
| A   | 2           | vlan2     | 10.2.2.3                                  |
| B   | 3           | vlan3     | 10.3.3.3                                  |
| C   | 4           | vlan4     | 10.4.4.3                                  |
| D   | 5           | vlan5     | 10.5.5.3                                  |
| E   | 6           | vlan6     | 10.6.6.3                                  |
| F   | 7           | vlan7     | 10.7.7.3                                  |
| G   | 8           | vlan8     | 10.8.8.3                                  |
| H   | 9           | vlan9     | 10.9.9.3                                  |
| I   | 10          | vlan10    | 10.10.10.3                                |
| J   | 11          | vlan11    | 10.11.11.3                                |
| K   | 12          | vlan12    | 10.12.12.3                                |
| L   | 13          | vlan13    | 10.13.13.3                                |

Complete the following steps to configure separate VLANs on your workgroup switch:

**Step 1** Using the VLAN assignment chart, create the VLAN *only* for your pod.

What command do you use to create a VLAN on your switch?

---

**Step 2** Verify that the correct VLAN has been added.

**Step 3** Set the workgroup router port (port e0/2) of the switch to your assigned VLAN number.

What command do you use to set the port to your assigned VLAN number?

---

**Step 4** Enter the proper **show** command to verify that port e0/2 is now in the correct VLAN.

**Step 5** Access the console port of your workgroup router **wg\_ro\_x**, where **x** is the pod letter assigned to you for this lab exercise.

**Step 6** From your workgroup router, enter interface configuration mode for your first Ethernet interface.

- Step 7** Change the Ethernet interface IP address to 10.x.x.12/24, where x is the VLAN number of the VLAN you created.
- Step 8** Create a static default route on your workgroup router that points to the core router using the **ip route 0.0.0.0 0.0.0.0 10.x.x.3** command, where x.x is your assigned VLAN number.

---

**Note** You will learn more about the **ip route** command later in this course.

---

- Step 9** Exit global configuration mode.
- Step 10** Enter the **show ip interface ethernet** command to verify the setting of your workgroup router IP address.
- Step 11** Verify that your workgroup router IP address is set to 10.x.x.12. (The mask is 255.255.255.0.)
- Step 12** Use the **ping 10.x.x.3** command from EXEC mode to verify connectivity from your workgroup router to the core router. The core router has ISL trunking configured and your instructor has already configured it to be in all the VLANs.

The address that you need to use to ping the core router from your workgroup router is 10.x.x.3, where x.x is the VLAN number of the VLAN you created.

What was the response from the core router?

- 
- Step 13** From your workgroup router, ping the core router at 10.1.1.3 (core router VLAN 1 IP address) to test interVLAN connectivity.
- Step 14** Proceed to Task 4.

## Task 4: Configure the Spanning Tree Protocol

In this task, you will configure the second trunk port on your workgroup switch to trunk to core\_sw\_b and observe the STP convergence when a loop is built.

Complete the following steps to configure the STP on your workgroup switch:

---

|             |                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The vty password for the core switches is "cisco", the IP address for core_sw_a is 10.1.1.2, and the IP address for core_sw_b is 10.1.1.4. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|

---

**Step 1** Have the instructor ensure that the interface on core\_sw\_b connecting to your workgroup switch (fa0/27) is operational. The instructor may need to enter the **no shutdown** command on this interface.

**Step 2** Set the port fa0/27 at your workgroup switch to trunk mode.

What command do you use to set the port to trunk mode?

---

What command do you use to display a trunk configuration?

---

**Step 3** Enter the command to determine the spanning-tree state of the VLAN you created earlier.

Which ports are in the forwarding state for the VLAN you created?

---

---

|             |                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Port e0/1 and ports fa0/26 and fa0/27 should all be in the forwarding state at your workgroup switch. |
|-------------|-------------------------------------------------------------------------------------------------------|

---

**Step 4** From your workgroup router, connect to core\_sw\_a and core\_sw\_b via Telnet and use the **show spantree vlan#** command to determine the spanning-tree state of the VLAN you created earlier.

Is the port on one of the core switches where your workgroup switch is connected in the blocking state? Refer to the table in this Exercise Preparation section of this lab exercise for the connection at the core switches.

---

What is the MAC address of the root bridge for the VLAN you created earlier?

---

Which switch is the root bridge?

---

What is the priority of the root bridge?

---

---

**Note** Port fa0/x (x is the port on which your workgroup switch is connected) on core\_sw\_b should be in the blocking state. The Catalyst 1900 series switches calculate a cost of 10 for the Fast Ethernet link, while other switches, including the Catalyst 2900 series XL switch if used in the core, calculate a cost of 19 for the Fast Ethernet link. Therefore, because of the lower cost, STP will prefer the path through the Catalyst 1900 series switch.

---

---

**Note** Core switch A should be the root bridge because your instructor manually set its bridge priority to a value of 0.

---

**Step 5** Open two active console sessions: one to the workgroup switch and one to the workgroup router. (Open two Telnet sessions to the terminal server to accomplish this step.)

**Step 6** From the command-line interface (CLI) prompt on your workgroup router, perform an extended ping to the core router using a ping count of 50,000.

---

**Note** You should see continuous successful ping replies from the core router. The current path from your switch to the core router should be via your FastEthernet0/26 port. If not, do not proceed to the next step; instead, troubleshoot the problem or ask your instructor for help.

---

**Step 7** At your switch, shut down the interface FastEthernet0/26.

What happened to the continuous ping to the core router?

---



---

|             |                                                                                                                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The ping should fail, then work again, after about 30 seconds. Is the ping successful after 30 seconds? If not, do not proceed to the next step; instead, troubleshoot the problem or ask your instructor for help. |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Step 8** At your switch, use **no shutdown** on interface FastEthernet0/26.

What happened to the continuous ping to the core router?

---

Is the ping successful after 30 seconds?

---

---

|             |                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The ping should fail, then work again, after about 30 seconds. If not, troubleshoot the problem or ask your instructor for help. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|

---

**Step 9** Stop the extended ping from your workgroup router to the core router by pressing **Ctrl-Shift-6** and then **Ctrl-Shift-6** again.

**Step 10** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You configured your switch in a VTP domain in the transparent mode.
- You configured your workgroup switch to trunk to the core\_sw\_a.
- You configured a VLAN on your switch and assigned the VLAN to the switch port that connects to your workgroup router.

# Catalyst 2950 Series Switch Lab Exercise Instructions

In this exercise, you will configure your workgroup switch to participate in a VTP domain in the transparent mode. This will prevent VLAN changes made on the workgroup switch from propagating to other switches in the lab.

Your instructor has configured the core switches to trunk to the workgroup switches from their previous nontrunking mode. This effectively prevents frames from passing between the core switches and the workgroup switches, blocking your access to the core devices.

You will configure trunking on one of the trunk ports so that you can reach the core router again. You will also configure a VLAN for the switch port that is connected to your workgroup router and change the IP address of the first Ethernet interface on your workgroup router. The new address is one that is in the VLAN assigned to your pod and can only reach other devices in the workgroup (in a different VLAN) via the core router.

Your instructor has configured the core router to support interVLAN routing. Finally, you will configure the second trunk port on your workgroup switch for trunking to core\_sw\_b and observe the STP convergence when a loop is built.

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                                               | Description                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ping &lt;CR&gt;</code>                                          | If an extended <b>ping</b> command is used, you will set the ping count manually. (Use this command in privileged EXEC mode.)                                                                                                                              |
| <code>interface interface<br/>switchport mode trunk</code>            | Sets a Fast Ethernet or Gigabit Ethernet port to trunk mode.                                                                                                                                                                                               |
| <code>interface interface<br/>switchport access vlan<br/>vlan#</code> | Assigns a port to a VLAN.                                                                                                                                                                                                                                  |
| <code>ping ip-address</code>                                          | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>show interface interface</code>                                 | Displays the trunk parameters.                                                                                                                                                                                                                             |
| <code>show spanning-tree vlan<br/>vlan#</code>                        | Displays spanning-tree information for a particular VLAN.                                                                                                                                                                                                  |
| <code>show interfaces interface<br/>switchport</code>                 | Displays VLAN and trunk information.                                                                                                                                                                                                                       |
| <code>show vlan</code>                                                | Displays information on all configured VLANs.                                                                                                                                                                                                              |
| <code>show vtp status</code>                                          | Displays the VTP status.                                                                                                                                                                                                                                   |
| <code>shutdown/no shutdown</code>                                     | Disables or enables an interface.                                                                                                                                                                                                                          |
| <code>vlan database</code>                                            | Enters the VLAN configuration mode.                                                                                                                                                                                                                        |
| <code>vlan vlan# name vlan-name</code>                                | Defines a VLAN and VLAN name.                                                                                                                                                                                                                              |
| <code>vtp {server   client  <br/>transparent}</code>                  | Sets the VTP mode; use the <b>no</b> form of this command to return to the default setting.                                                                                                                                                                |
| <code>vtp domain domain</code>                                        | Sets the VTP administrative domain.                                                                                                                                                                                                                        |

## Task 1: Configure VTP and VTP Domains

In this exercise, you will configure your workgroup switch to participate in a VTP domain in the transparent mode. This will prevent VLAN changes made on the workgroup switch from propagating to other switches in the lab.

Complete the following steps on your workgroup switch:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup switch from the Pod menu.
- Step 4** Enter privileged EXEC mode using the **enable** command.
- Step 5** Shut down the fa 0/12 interface on your workgroup switch.
- Step 6** Set the VTP domain name to “ICND” and the mode to transparent.

What command sequence do you use to set the domain name and VTP mode on your workgroup switch?

- 
- Step 7** Verify the VTP configuration using the **show vtp status** command. Your output should look similar to the following display:

```
wg_sw_z#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 68
Number of existing VLANs : 5
VTP Operating Mode : Transparent
VTP Domain Name : ICND
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xCB 0x48 0xFA 0x38 0xE2
 0x34 0x95 0xC2
Configuration last modified by 10.1.1.10 at 3-2-93 13:40:28
```

Is the domain name the same that you entered? Are you in transparent mode?

- 
- Step 8** Proceed to Task 2.

## Task 2: Assign a Switch to the Appropriate VTP Mode

The instructor has configured the core switches to trunk to the workgroup switches from their previous nontrunking mode. This configuration effectively shuts off frames from passing between the core switches and the workgroup switches and blocks your access to the core devices. You will configure trunking on one of the trunk ports so that you can reach the core router again.

Complete the following steps to configure trunking mode on your workgroup switch:

**Step 1** Set the port fa0/11 at your workgroup switch to trunk mode.

What command do you use to set the port to trunk mode?

---

**Step 2** Verify the trunk configuration.

What command do you use to display a trunk configuration?

---

Your output should look similar to the following display:

```
wg_sw_a#show interface FastEthernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

**Step 3** To verify trunking, ping the core router at 10.1.1.3 from the workgroup switch. (If it does not work, make sure that your fa 0/12 interface is shut down.)

**Step 4** Proceed to Task 3.

### Task 3: Configure Separate VLANs on the Switch

In this task, you will configure a VLAN for the switch port that is connected to your workgroup router and change the IP address of the first Ethernet interface on your workgroup router. The new address is one that is in the VLAN assigned to your pod and can only reach other devices in the workgroup (in a different VLAN) via the core router. Your instructor has configured the core router to support interVLAN routing.

The table, or VLAN assignment chart, provides information you need to complete this task.

| Pod | VLAN Number | VLAN Name | core_ro_x<br>(where x is your<br>pod letter) | wg_ro_x e0/0<br>(where x is your<br>pod letter) |
|-----|-------------|-----------|----------------------------------------------|-------------------------------------------------|
| A   | 2           | vlan2     | 10.2.2.3                                     | 10.2.2.12                                       |
| B   | 3           | vlan3     | 10.3.3.3                                     | 10.3.3.12                                       |
| C   | 4           | vlan4     | 10.4.4.3                                     | 10.4.4.12                                       |
| D   | 5           | vlan5     | 10.5.5.3                                     | 10.5.5.12                                       |
| E   | 6           | vlan6     | 10.6.6.3                                     | 10.6.6.12                                       |
| F   | 7           | vlan7     | 10.7.7.3                                     | 10.7.7.12                                       |
| G   | 8           | vlan8     | 10.8.8.3                                     | 10.8.8.12                                       |
| H   | 9           | vlan9     | 10.9.9.3                                     | 10.9.9.12                                       |
| I   | 10          | vlan10    | 10.10.10.3                                   | 10.10.10.12                                     |
| J   | 11          | vlan11    | 10.11.11.3                                   | 10.11.11.12                                     |
| K   | 12          | vlan12    | 10.12.12.3                                   | 10.12.12.12                                     |
| L   | 13          | vlan13    | 10.13.13.3                                   | 10.13.13.12                                     |

Complete the following steps to configure separate VLANs on your workgroup switch:

**Step 1** Using the VLAN assignment chart, create the VLAN *only* for your pod.

What command do you use to create a VLAN on your switch?

---

**Step 2** Verify that the correct VLAN has been added using the **show vlan** command from the EXEC mode.

**Step 3** Set the workgroup router port (port fa0/2) of the switch to your assigned VLAN number.

What command do you use to set the port to your assigned VLAN number?

---

**Step 4** Enter the proper **show** command to verify that port fa0/2 is now in the correct VLAN.

**Step 5** Access the console port of your workgroup switch **wg\_ro\_x**, where **x** is the pod letter assigned to you for this lab exercise.

**Step 6** From your workgroup router, enter interface configuration mode for your first Ethernet interface.

**Step 7** Change the primary Ethernet interface in your workgroup router to 10.x.x.12 (where x is your assigned VLAN number) and assign a subnet mask of 255.255.255.0.

**Step 8** Ping the core router at 10.x.x.3, where x is your assigned VLAN number, from your workgroup router.

Your ping should be successful. Why?

---

**Step 9** Ping your workgroup switch from your workgroup router.

Your ping should *not* be successful. Why?

---

**Step 10** Enable interVLAN communications by configuring a default route on your workgroup router that points to the core router using the **ip route 0.0.0.0 0.0.0.0 10.x.x.3** command, where x.x is your assigned VLAN number. Now ping your workgroup switch.

Your ping should be successful? Why?

---

**Step 11** Verify that the default gateway on your workgroup switch is set to 10.1.1.3 so your workgroup switch can ping devices in other VLANs via the core router.

**Step 12** Proceed to Task 4.

#### Task 4: Configure the Spanning Tree Protocol

In this task, you will configure the second trunk port on your workgroup switch to trunk to core\_sw\_b and observe the STP convergence when a loop is built.

Complete the following steps to configure the STP on your workgroup switch:

---

**Note** The vty password for the core switches is "cisco", the IP address for core\_sw\_a is 10.1.1.2, and the IP address for core\_sw\_b is 10.1.1.4.

---

**Step 1** Have the instructor verify that the interface on core\_sw\_b connecting to your workgroup switch is configured properly for trunking. (The instructor may need to enter the **no shutdown** command on this interface.) Make sure the fa 0/12 interface at your workgroup switch is still shut down.

**Step 2** Set the port fa0/12 at your workgroup switch to trunk mode.

What command do you use to set the port to trunk mode?

---

What command do you use to display a trunk configuration?

---

- Step 3** Enter the **no shutdown** command on the fa 0/12 interface on your workgroup switch.
- Step 4** Enter the command to determine the spanning-tree state of the VLAN you created earlier.

Which ports are in the forwarding state for the VLAN you created?

---

---

**Note** Port fa0/2 and port fa0/11 should be in the forwarding state on your workgroup switch.

---

- Step 5** From the **show spanning-tree vlan x** command output on the core switches and your workgroup switch, determine which port is in the blocking state.

- Step 6** What is the MAC address of the root bridge for the VLAN you created earlier? Which switch is the root bridge? What is the priority of the root bridge?

---

---

**Note** Core switch A should be the root bridge because the bridge priority is manually set to a value of 0 by your instructor.

---

- Step 7** Open two active console sessions: one to the workgroup switch and one to the workgroup router. (Open two Telnet sessions to the terminal server to accomplish this step.)

- Step 8** From the console session on the workgroup router, perform an extended ping to the core router (10.x.x.3, where x is your assigned VLAN number) with a count of 50,000.

Is the ping successful?

---

---

**Note** You should see continuous successful ping replies from the core router. The current path from your switch to the core router should be via your FastEthernet0/11 port. If not, do not proceed to the next step; instead, troubleshoot the problem or ask your instructor for help.

---

- Step 9** At your switch, no shut the interface FastEthernet0/11.

What happened to the extended ping to the core router?

---

Is the ping successful after 30 seconds?

---



---

|             |                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | The ping should fail, then work again, after about 30 seconds. If not, troubleshoot the problem or ask your instructor for help. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|

---

**Step 10** Stop the extended ping from your workgroup router to the core router by pressing **Ctrl-Shift-6** and then **Ctrl-Shift-6** again.

**Step 11** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You successfully pinged the core router from your workgroup router.
- You successfully pinged devices in a different VLAN from your workgroup router.
- You determined the spanning-tree state for the VLAN you created when the STP closed the loop that you created by putting one of the uplink ports into blocked mode.

# Lab Exercise 3-1: Determining IP Routes with RIP

Complete the lab exercise to practice what you learned in this module.

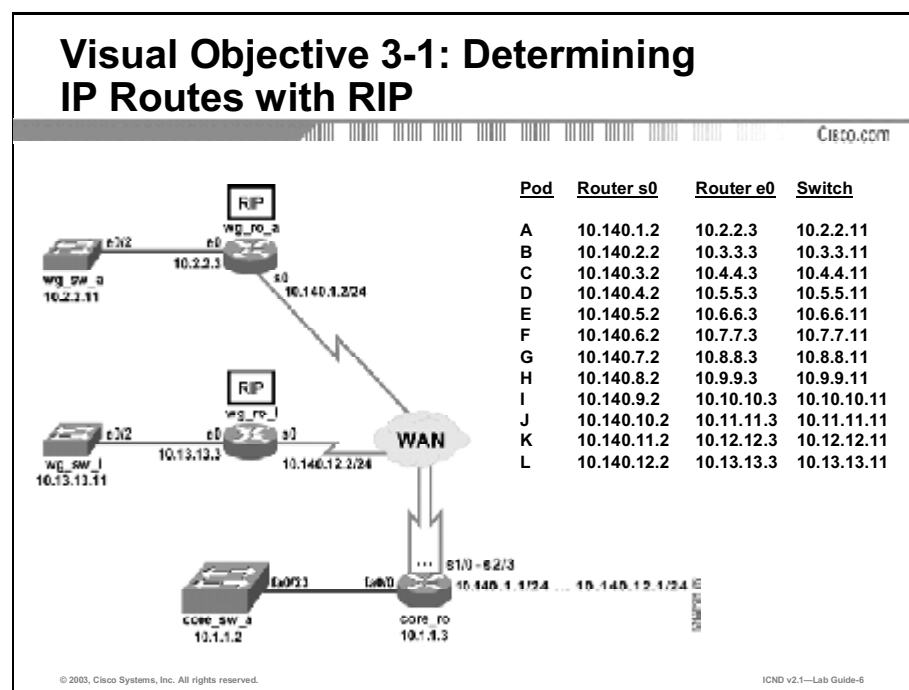
## Exercise Objective

Given a remote workgroup router and core office router with serial cables connecting both sites, you will place the workgroup and core routers in separate LANs connected by a serial connection. You will also configure the serial interface of the workgroup router and enable the Routing Information Protocol (RIP) to dynamically learn about the core network so you can ping to the core router via the serial connection. After completing this exercise, you will be able to meet these objectives:

- Set up LAN connections from a workgroup to a core site
- Enable serial connections from a workgroup router to a core site
- Enable and verify routing with RIP

## Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

### Catalyst 1900 Series Commands

| Command                                    | Description                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip address ip-address mask</code>    | Defines the IP address and subnet mask for the Catalyst switch.                                                                                                                                                                                            |
| <code>ip default-gateway ip-address</code> | Defines a default gateway on the Catalyst switch.                                                                                                                                                                                                          |
| <code>no ip route</code>                   | Turns off a static route.                                                                                                                                                                                                                                  |
| <code>ping ip-address</code>               | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>show ip</code>                       | Displays the IP configuration on the Catalyst switch.                                                                                                                                                                                                      |
| <code>show ip protocol</code>              | Displays information about the configured and run-time IP parameters and IP routes.                                                                                                                                                                        |
| <code>show vlan-membership</code>          | Displays VLAN membership information on the Catalyst switch.                                                                                                                                                                                               |
| <code>shutdown/no shutdown</code>          | Disables or enables an interface.                                                                                                                                                                                                                          |
| <code>vlan-membership static 1</code>      | Defines the VLAN membership of an interface on the Catalyst switch.                                                                                                                                                                                        |

### Catalyst 2950 Series Commands

| Command                                                                 | Description                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>interface vlan1</code><br><code>ip address ip-address mask</code> | Defines the IP address and subnet mask for the Catalyst switch.                                                                                                                                                                                            |
| <code>ip default-gateway ip-address</code>                              | Defines a default gateway on the Catalyst switch.                                                                                                                                                                                                          |
| <code>ping ip-address</code>                                            | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>show interfaces vlan 1</code>                                     | Displays IP configuration on the Catalyst switch.                                                                                                                                                                                                          |
| <code>show vlan</code>                                                  | Displays VLAN membership information on the Catalyst switch.                                                                                                                                                                                               |
| <code>switchport access vlan 1</code>                                   | Defines the VLAN membership of VLAN interfaces on the Catalyst 2950 series switch.                                                                                                                                                                         |

## Cisco Router Commands

| Command                                    | Description                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>debug ip rip</code>                  | Displays routing updates as they are sent and received.                                                                                                                                                                                                    |
| <code>line console 0</code>                | Enables the user role and password.                                                                                                                                                                                                                        |
| <code>network <i>network-number</i></code> | Starts up the routing protocol on all interfaces that the router has in the specified network.                                                                                                                                                             |
| <code>no debug all</code>                  | Turns off all debugging displays.                                                                                                                                                                                                                          |
| <code>router rip</code>                    | Enables the routing process with RIP.                                                                                                                                                                                                                      |
| <code>ping <i>ip-address</i></code>        | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>show ip protocols</code>             | Displays values about routing protocols and routing protocol timer information associated with the router.                                                                                                                                                 |
| <code>show ip route</code>                 | Displays the IP routing table.                                                                                                                                                                                                                             |

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

In this exercise, you will use the default encapsulation for a serial link, High-Level Data Link Control (HDLC), to distribute routing protocol traffic from your workgroup to the core. This requires shutting down the uplinks to the core switches on your workgroup switch. You will also assign an IP address to your first serial interface. Your last step is to enable RIP and verify its operation.

For the remaining lab exercises, communications with the core will be via the WAN connection. If you are not using a remote lab, make sure that the physical serial connection is correctly attached from your workgroup router to the service provider. The core router simulates the service provider for this exercise.

Your instructor will place the core network into a separate network, 10.1.1.0.

The table lists the addresses that you will use in this lab exercise.

| Workgroup | IP Address for Workgroup Switch (Example: wg_sw_x) | Workgroup Router Ethernet 0 Interface (wg_ro_x) | Serial0 on Workgroup Router (wg_ro_x) | Core Router Serial Interface Address (core_ro) |
|-----------|----------------------------------------------------|-------------------------------------------------|---------------------------------------|------------------------------------------------|
| A         | 10.2.2.11/24                                       | 10.2.2.3/24                                     | 10.140.1.2/24                         | 10.140.1.1/24                                  |
| B         | 10.3.3.11/24                                       | 10.3.3.3/24                                     | 10.140.2.2/24                         | 10.140.2.1/24                                  |
| C         | 10.4.4.11/24                                       | 10.4.4.3/24                                     | 10.140.3.2/24                         | 10.140.3.1/24                                  |
| D         | 10.5.5.11/24                                       | 10.5.5.3/24                                     | 10.140.4.2/24                         | 10.140.4.1/24                                  |
| E         | 10.6.6.11/24                                       | 10.6.6.3/24                                     | 10.140.5.2/24                         | 10.140.5.1/24                                  |
| F         | 10.7.7.11/24                                       | 10.7.7.3/24                                     | 10.140.6.2/24                         | 10.140.6.1/24                                  |
| G         | 10.8.8.11/24                                       | 10.8.8.3/24                                     | 10.140.7.2/24                         | 10.140.7.1/24                                  |
| H         | 10.9.9.11/24                                       | 10.9.9.3/24                                     | 10.140.8.2/24                         | 10.140.8.1/24                                  |
| I         | 10.10.10.11/24                                     | 10.10.10.3/24                                   | 10.140.9.2/24                         | 10.140.9.1/24                                  |
| J         | 10.11.11.11/24                                     | 10.11.11.3/24                                   | 10.140.10.2/24                        | 10.140.10.1/24                                 |
| K         | 10.12.12.11/24                                     | 10.12.12.3/24                                   | 10.140.11.2/24                        | 10.140.11.1/24                                 |
| L         | 10.13.13.11/24                                     | 10.13.13.3/24                                   | 10.140.12.2/24                        | 10.140.12.1/24                                 |

## Task 1: Set Up LAN Connections from the Workgroup to the Core

This step requires that you shut down the LAN connection from your workgroup to the core. You will also change the IP address on your workgroup switch and the first Ethernet interface on your router.

Complete the following steps to place the workgroup and core in the separate LANs that are connected via a serial connection:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup switch from the Pod menu.
- Step 4** Enter global configuration mode.
- Step 5** Shut down the ports (fa 0/11 and fa 0/12) to the core\_sw\_a and core\_sw\_b switches.
- Step 6** Change the IP address on the workgroup switch, wg\_sw\_x, where x is your pod letter, to the address listed in the Exercise Preparation topic for this lab exercise.
- Step 7** Change the default gateway on the switch to be the wg\_ro\_x Ethernet interface, where x is the letter for your pod. For example, for pod A, the default gateway for the workgroup switch is 10.2.2.3.
- Step 8** Change the interface connected to wg\_ro\_x, where x is the letter for your pod, to VLAN 1 by entering interface configuration mode and issuing the appropriate command.
- Step 9** Exit global configuration mode.
- Step 10** Enter the **show ip** command (on the Catalyst 1900 series) or the **show interface vlan 1** command (on the Catalyst 2950 series) to verify that you configured the correct IP address.
- Step 11** Show the running configuration to verify that the default gateway is properly configured.
- Step 12** Enter the proper **show** command to verify that the interface to workgroup router interface is now in VLAN 1.
- Step 13** Move to your workgroup router console connection. On the workgroup router, change the address on the workgroup router Ethernet interface to the address listed in the Exercise Preparation topic for this lab exercise.
- Step 14** From your workgroup router, ping your workgroup switch to test connectivity. The ping should be successful.
- Step 15** Proceed to Task 2.

## Task 2: Enable a Serial Connection from the Workgroup Router to the Core Site

This task requires that you remove the default route configured previously on the router, assign an IP address to your first serial interface, and verify that you cannot reach the core router IP address of 10.1.1.3. You will establish connectivity in the next task.

Complete the following steps on the workgroup router to enable a serial connection:

- Step 1** Enter global configuration mode.
- Step 2** Remove the default route using the **no ip route 0.0.0.0 0.0.0.0 10.x.x.3** command, which you configured in an earlier lab.
- Step 3** Enter interface configuration mode and assign an IP address to the first serial interface. Refer to the Exercise Preparation topic of this lab exercise for the correct IP address. For example, for pod A, the address is 10.140.1.2.
- Step 4** Exit global configuration mode.
- Step 5** Ping the core router serial interface directly connected to your serial network. Refer to the Exercise Preparation topic of this lab exercise for the correct IP address. For example, for pod A, the address is 10.140.1.1.  
The ping should work. Why?

- 
- Step 6** Ping the core router at 10.1.1.3.  
The ping did not work. Why not?

- 
- Step 7** View your IP routing table to see all paths listed in the table. Which command do you enter to view the IP routing table? Your output should look similar to the following display:

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

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

```
 10.0.0.0/24 is subnetted, 2 subnets
C 10.2.2.0 is directly connected, Ethernet0
C 10.140.1.0 is directly connected, Serial0
wg_ro_z#
```

- Step 8** Proceed to Task 3.

## Task 3: Enable and Verify Routing with RIP

In this topic, you will enable RIP on your router. After RIP is enabled, has sent and received updates, and has populated its next-hop forwarding table (routing table), you will be able to reach IP addresses not on your network, such as the core router 10.1.1.3 address.

Complete the following steps on the workgroup router to route with the RIP protocol:

- Step 1** Enter global configuration mode.
- Step 2** Enable the RIP routing protocol.
- Step 3** Enter the network numbers for all networks that are directly connected to your router. In this lab exercise, the entire network is in the 10.0.0.0 network.
- Step 4** Exit global configuration mode.
- Step 5** Verify that the RIP routing protocol is enabled and that the networks you identified in the previous step are recognized by RIP with the **show ip protocol** command. Your output should look similar to the following display:

```
wg_ro_z#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 20 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 1, receive any version
 Interface Send Recv Key-chain
 Ethernet0 1 1 2
 Serial0 1 1 2
 Routing for Networks:
 10.0.0.0
 Routing Information Sources:
 Gateway Distance Last Update
 10.140.1.1 120 00:00:01
 Distance: (default is 120)
```

- Step 6** To display the current state of the routing table, enter the **show ip route** command. Your output should look similar to the following display where you will also see routes from any other pods that are configured for RIP:

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

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 8 subnets
R 10.1.1.0 [120/1] via 10.140.1.1, 00:00:16, Serial0
```



```
C 10.2.2.0 is directly connected, Ethernet0
C 10.140.1.0 is directly connected, Serial0
```

In the RIP routing table display, how do you determine which networks are discovered by the RIP routing protocol?

---

**Step 7** Display the RIP routing updates sent from and received at your router with the **debug ip rip** command. Your output should look similar to the following display where you will see updates for your pod and other pods:

```
wg_ro_z#debug ip rip
RIP protocol debugging is on
wg_sw_z#
22:11:21: RIP: sending v1 update to 255.255.255.255 via
Ethernet0 (10.2.2.3)
22:11:21: subnet 10.1.1.0, metric 2
22:11:21: subnet 10.140.1.0, metric 1
22:11:21: RIP: sending v1 update to 255.255.255.255 via
Serial0 (10.140.1.2)
22:11:21: subnet 10.2.2.0, metric 1
22:11:35: RIP: received v1 update from 10.140.1.1 on Serial0
22:11:35: 10.1.1.0 in 1 hops
```

**Step 8** Disable the display of the RIP routing updates sent from and received at your router and all other debugging.

**Step 9** Ping the core router at 10.1.1.3.

Can you successfully reach the core router?

---

**Step 10** Return to privileged EXEC mode and log out of your router.

**Step 11** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You were able to learn the route to the core router with the RIP routing protocol.
- You were able to ping the core router using the dynamically learned route via the serial connection.

# Lab Exercise 3-2: Determining IP Routes with IGRP

Complete the lab exercise to practice what you learned in this module.

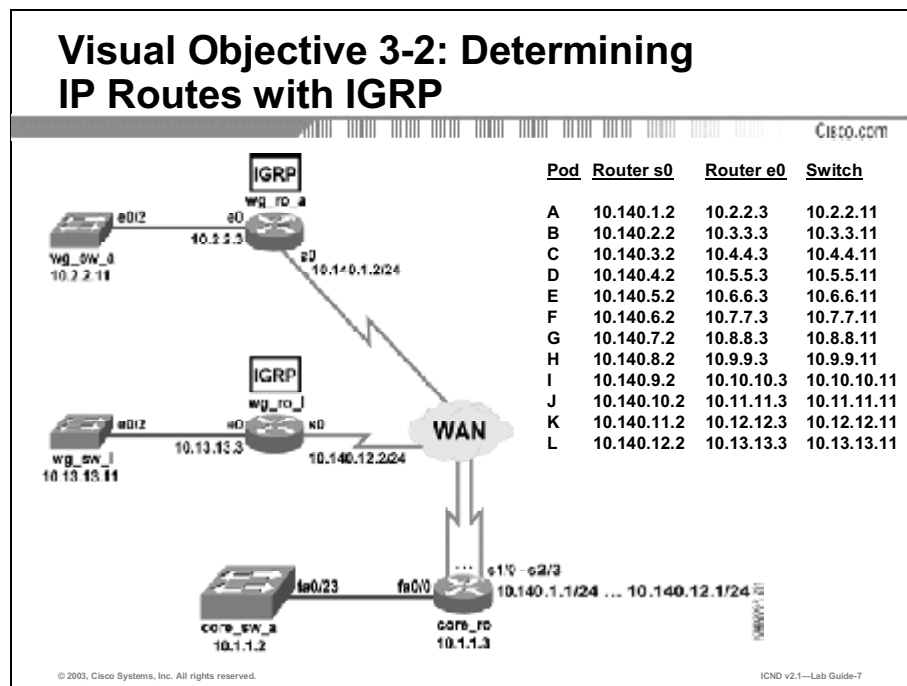
## Exercise Objective

Given a remote workgroup router and core office router with serial cables connecting both sites, you will enable the Interior Gateway Routing Protocol (IGRP) to dynamically learn about the core network so that you can ping to the core router via the serial connection. After completing this exercise, you will be able to meet these objectives:

- Enable routing with IGRP
- Verify routing with IGRP
- Debug routing with IGRP

## Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                    | Description                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>debug ip igrp events</code>          | Displays a summary of IGRP transaction information.                                                                                                                                                                                                        |
| <code>debug ip igrp transactions</code>    | Displays IGRP transaction information.                                                                                                                                                                                                                     |
| <code>debug ip rip</code>                  | Displays routing updates as they are sent and received.                                                                                                                                                                                                    |
| <code>network network-number</code>        | Starts up the routing protocol on all interfaces that the router has in the specified network.                                                                                                                                                             |
| <code>no debug all</code>                  | Turns off all debugging displays.                                                                                                                                                                                                                          |
| <code>no router rip</code>                 | Disables RIP routing.                                                                                                                                                                                                                                      |
| <code>ping ip-address</code>               | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <code>router igrp autonomous-system</code> | Enables the IGRP routing protocol.                                                                                                                                                                                                                         |
| <code>show ip protocols</code>             | Displays values about routing protocols and routing protocol timer information associated with the router.                                                                                                                                                 |
| <code>show ip route</code>                 | Displays the IP routing table.                                                                                                                                                                                                                             |

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

The purpose of this lab is to give you experience in configuring, verifying, and debugging the IGRP routing protocol. The lab begins with RIP still running on both your workgroup and core routers. You should have full connectivity with RIP.

You will configure IGRP and verify that the routes you learn on your workgroup router are learned through IGRP, illustrating how even though two routing protocols are running, only the best and most trustworthy route is put in the routing table. The last steps you complete will be to see the debug reports of a router running IGRP to help you better understand the protocol and assist you when you need to troubleshoot IGRP.

The table lists addresses you will use in this lab exercise.

| Workgroup | Workgroup Router Ethernet 0 Interface (wg_ro_x) | IP Address for Workgroup Switch (Example: wg_sw_x) | First Serial Interface on Workgroup Router (wg_ro_x) | Core Router's Serial Interface Address (core_ro) |
|-----------|-------------------------------------------------|----------------------------------------------------|------------------------------------------------------|--------------------------------------------------|
| A         | 10.2.2.3                                        | 10.2.2.11                                          | 10.140.1.2                                           | 10.140.1.1                                       |
| B         | 10.3.3.3                                        | 10.3.3.11                                          | 10.140.2.2                                           | 10.140.2.1                                       |
| C         | 10.4.4.3                                        | 10.4.4.11                                          | 10.140.3.2                                           | 10.140.3.1                                       |
| D         | 10.5.5.3                                        | 10.5.5.11                                          | 10.140.4.2                                           | 10.140.4.1                                       |
| E         | 10.6.6.3                                        | 10.6.6.11                                          | 10.140.5.2                                           | 10.140.5.1                                       |
| F         | 10.7.7.3                                        | 10.7.7.11                                          | 10.140.6.2                                           | 10.140.6.1                                       |
| G         | 10.8.8.3                                        | 10.8.8.11                                          | 10.140.7.2                                           | 10.140.7.1                                       |
| H         | 10.9.9.3                                        | 10.9.9.11                                          | 10.140.8.2                                           | 10.140.8.1                                       |
| I         | 10.10.10.3                                      | 10.10.10.11                                        | 10.140.9.2                                           | 10.140.9.1                                       |
| J         | 10.11.11.3                                      | 10.11.11.11                                        | 10.140.10.2                                          | 10.140.10.1                                      |
| K         | 10.12.12.3                                      | 10.12.12.11                                        | 10.140.11.2                                          | 10.140.11.1                                      |
| L         | 10.13.13.3                                      | 10.13.13.11                                        | 10.140.12.2                                          | 10.140.12.1                                      |

## Task 1: Enable Routing with IGRP

For this task, you will enable routing with IGRP.

Complete the following steps on the workgroup router:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main Menu appears.
- Step 2** Select your workgroup from the Main Menu. The Pod Menu appears.
- Step 3** Select your workgroup router from the Pod Menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Verify that RIP is configured on the core router by using the **show ip route** command. You should be learning the route to the core router via your first serial interface.
- Step 5** Verify that all subnet masks you are using with your workgroup IP addresses are set to 255.255.255.0.
- Step 6** Enter global configuration mode.
- Step 7** Enable the IGRP routing protocol. Use the value 200 for your autonomous system number.
- Step 8** Enter the network numbers for all networks directly connected to your router. In this lab exercise, the entire network is in the 10.0.0.0 network.
- Step 9** Exit global configuration mode.
- Step 10** Proceed to Task 2.

## Task 2: Verify Routing with IGRP

In this topic, you will verify that IGRP routing is working correctly.

Complete the following steps on the workgroup router to verify IGRP operation:

- Step 1** Verify that the core subnet route 10.1.1.0, learned from RIP, is now being replaced by the IGRP routing protocol. Your output should be similar to the following display:

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

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

```
 10.0.0.0/24 is subnetted, 8 subnets
I 10.1.1.0 [100/8486] via 10.140.1.1, 00:00:22, Serial0
C 10.2.2.0 is directly connected, Ethernet0
C 10.140.1.0 is directly connected, Serial0
wg_ro_z#
```

What is the parameter that indicates that IGRP is a more trustworthy routing protocol than RIP?

---

If you disabled IGRP, would you lose connectivity to the 10.1.1.0 subnet? Why not?

---

- Step 2** Proceed to Task 3.

## Task 3: Debug Routing with IGRP

In this topic, you will debug IGRP routing.

Complete the following steps on the workgroup router to troubleshoot IGRP operation:

**Step 1** Use the **debug ip rip** command to answer the following questions:

Are you seeing RIP updates from the core router about subnet 10.1.1.0?

---

Why is the RIP router NOT populated in your routing table?

---

**Step 2** Enter the **show ip protocols** command to verify that the IGRP routing protocol is enabled and that the autonomous groups you assigned in the previous step are recognized by IGRP. You will also see that RIP is running. Your output should look similar to the following display:

```
wg_ro_z#show ip protocols
Routing Protocol is "igrp 200"
 Sending updates every 90 seconds, next due in 31 seconds
 Invalid after 270 seconds, hold down 280, flushed after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 200
 Routing for Networks:
 10.0.0.0
 Routing Information Sources:
 Gateway Distance Last Update
 10.140.1.1 100 00:00:25
 Distance: (default is 100)
```

**Step 3** Answer the following questions.

What is the administrative distance of IGRP?

---

What is the administrative distance of RIP?

---

Which administrative distance is better?

---

- Step 4** Display the IGRP routing update transactions sent from the router with the **debug ip igrp transactions** command. Your output should look similar to the following display:

```
wg_ro_z#debug ip igrp transactions
IGRP protocol debugging is on
wg_ro_z#
22:27:30: IGRP: sending update to 255.255.255.255 via
Ethernet0 (10.2.2.3)
22:27:30: subnet 10.1.1.0, metric=8486
22:27:30: subnet 10.140.1.0, metric=8476
22:27:31: IGRP: sending update to 255.255.255.255 via Serial0
(10.140.1.2)
22:27:31: subnet 10.2.2.0, metric=1100
22:27:40: IGRP: received update from 10.140.1.1 on Serial0
22:27:40: subnet 10.1.1.0, metric 8486 (neighbor 110)
```

- Step 5** Turn off the display of IGRP routing updates.
- Step 6** Turn off all debugging.
- Step 7** Ping the core router at 10.1.1.3.
- Step 8** Use the **no router rip** command to disable RIP routing.
- Step 9** Return to the privileged EXEC mode and save your running configuration to startup-config. You will need to use your IGRP configuration in later lab exercises.
- Step 10** Log out of your router.
- Step 11** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You were able to learn the route to the core router with the IGRP
- You were able to ping the core router using the dynamically learned route via the serial connection.



# Lab Exercise 3-3: Determining IP Routes with EIGRP

Complete the lab exercise to practice what you have learned in this module.

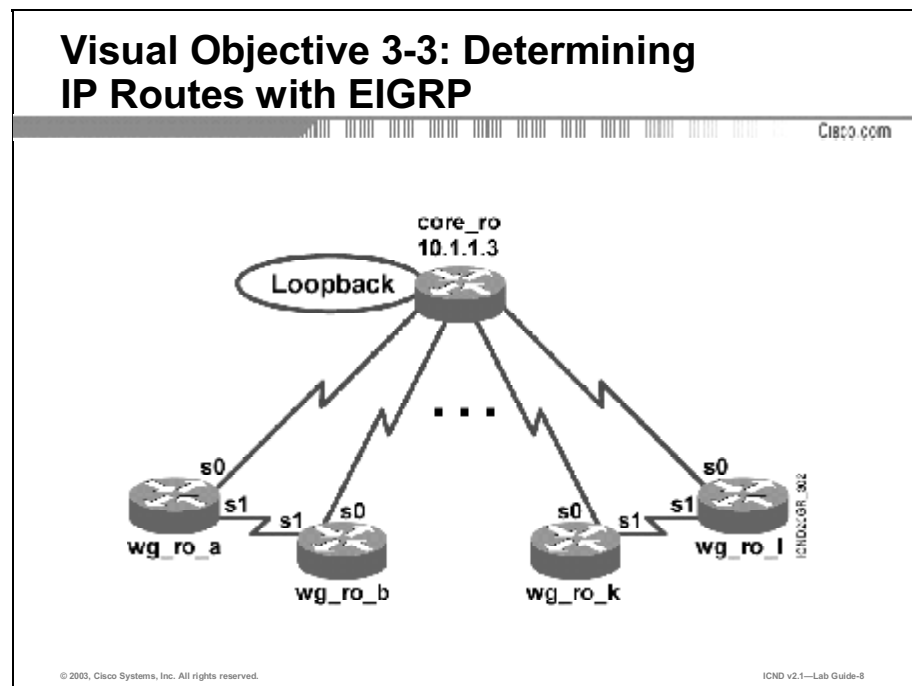
## Exercise Objective

Given a remote workgroup router and core office router with serial cables connecting both sites, you will enable the Enhanced Interior Gateway Routing Protocol (EIGRP) to dynamically learn about the core network so you can ping to the core router (10.1.1.3) via the serial connection. After completing this exercise, you will be able to meet these objectives:

- Enable routing with EIGRP
- Verify routing with EIGRP
- Debug routing with EIGRP

## Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                           | Description                                                                                                                                                                                                                                                |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>clock rate</b>                                 | Configures the clock rate on serial interfaces.                                                                                                                                                                                                            |
| <b>debug eigrp neighbors</b>                      | Displays EIGRP neighbors discovered by EIGRP.                                                                                                                                                                                                              |
| <b>ip address</b> <i>ip-address mask</i>          | Defines the IP address and subnet mask for an interface.                                                                                                                                                                                                   |
| <b>network</b> <i>network-number</i>              | Starts up the routing protocol on all the router interfaces that match the specified network.                                                                                                                                                              |
| <b>no debug all</b>                               | Turns off all debugging displays.                                                                                                                                                                                                                          |
| <b>no router igrp</b><br><i>autonomous-system</i> | Disables IGRP routing process.                                                                                                                                                                                                                             |
| <b>ping</b> <i>ip-address</i>                     | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <b>router eigrp</b><br><i>autonomous-system</i>   | Enables EIGRP.                                                                                                                                                                                                                                             |
| <b>show controllers</b>                           | Displays the controller state that is specific to the controller hardware.                                                                                                                                                                                 |
| <b>show interfaces</b>                            | Displays statistics for the interfaces configured on the router.                                                                                                                                                                                           |
| <b>show ip protocols</b>                          | Displays values about routing protocols and routing protocol timer information associated with the router.                                                                                                                                                 |
| <b>show ip route</b>                              | Displays the IP routing table.                                                                                                                                                                                                                             |

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

You have previously configured your network to route by using two *classful* routing protocols, RIP and IGRP. This lab exercise introduces you to the first of two *classless* routing protocols: EIGRP. This protocol is similar to IGRP in configuration and will actually coexist with IGRP if the two routing protocols are in the same autonomous system.

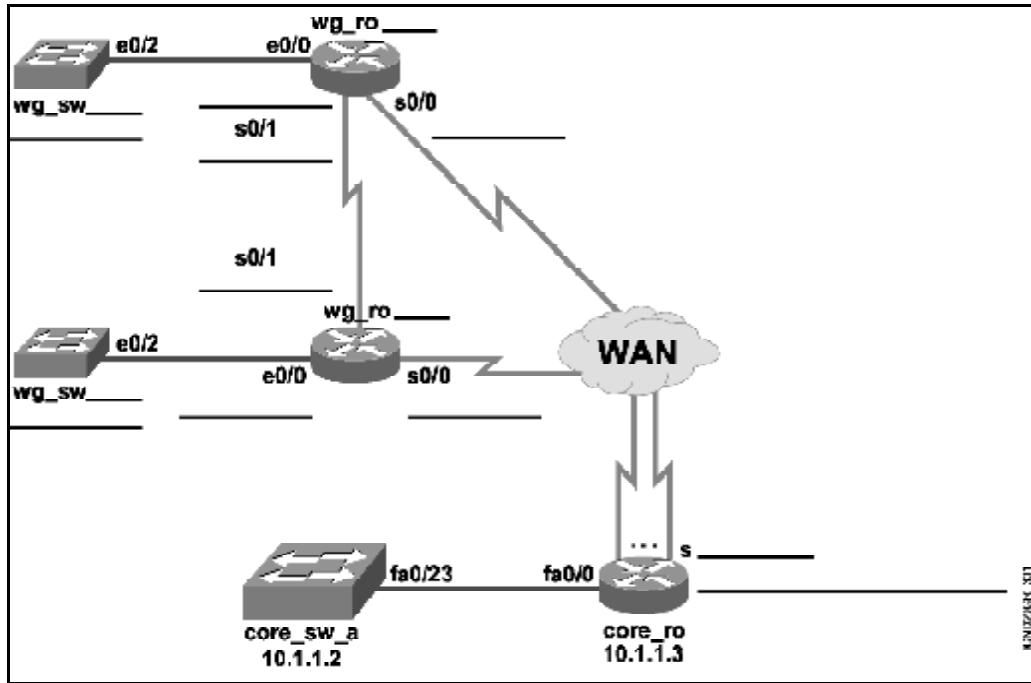
Your tasks in this lab are to change the address of your first serial interface, then to enable and address your second serial interface. In the Visual Objective, two pods are interconnected via a second serial link. When you configure this link, you will need to discover which side has the data circuit-terminating equipment (DCE) cable attached and provide a clock to synchronize the data transmission. You will use the default encapsulation, HDLC, to carry your data on this link between pods. When your serial links are up, you will configure EIGRP routing.

After you have EIGRP routing configured, you will verify the configuration and operation of the routing protocol. The last task you will complete is to debug the routing protocol so that you know what to look for when you need to troubleshoot EIGRP routing protocol issues.

The table lists the IP addresses that you will use in this lab exercise. Subnet masks are indicated with the */bits* designation to indicate the number of bits in the mask.

| Workgroup | Serial0 on Workgroup Router (wg_ro_x) | Serial1 on Workgroup Router (wg_ro_x) | Core Router Serial Interface Address (core_ro) | EIGRP Autonomous System Number |
|-----------|---------------------------------------|---------------------------------------|------------------------------------------------|--------------------------------|
| A         | 192.168.1.34/28                       | 192.168.1.17/28                       | 192.168.1.33/28                                | 100                            |
| B         | 192.168.1.50/28                       | 192.168.1.18/28                       | 192.168.1.49/28                                | 100                            |
| C         | 192.168.2.34/28                       | 192.168.2.17/28                       | 192.168.2.33/28                                | 200                            |
| D         | 192.168.2.50/28                       | 192.168.2.18/28                       | 192.168.2.49/28                                | 200                            |
| E         | 192.168.3.34/28                       | 192.168.3.17/28                       | 192.168.3.33/28                                | 300                            |
| F         | 192.168.3.50/28                       | 192.168.3.18/28                       | 192.168.3.49/28                                | 300                            |
| G         | 192.168.4.34/28                       | 192.168.4.17/28                       | 192.168.4.33/28                                | 400                            |
| H         | 192.168.4.50/28                       | 192.168.4.18/28                       | 192.168.4.49/28                                | 400                            |
| I         | 192.168.5.34/28                       | 192.168.5.17/28                       | 192.168.5.33/28                                | 500                            |
| J         | 192.168.5.50/28                       | 192.168.5.18/28                       | 192.168.4.49/28                                | 500                            |
| K         | 192.168.6.34/28                       | 192.168.6.17/28                       | 192.168.6.33/28                                | 600                            |
| L         | 192.168.6.50/28                       | 192.168.6.18/28                       | 192.168.6.49/28                                | 600                            |

You will work with a partner pod to complete this exercise. Use the previous table to enter the IP addresses for your router (and the router belonging to your partner), in the diagram below. Include the names of the devices in the blanks provided.



## Task 1: Enable Routing with EIGRP

Your tasks in this lab are to change the address of your first serial interface, then to enable and address your second serial interface. You will note from the Visual Objective that two pods are now interconnected via a second serial link. When you configure this link, you will need to discover which side has the DCE cable attached and provide a clock to synchronize the data transmission. You will use the default encapsulation, HDLC, to carry your data on this link between pods. When your serial links are up, you will configure EIGRP routing.

Complete the following steps on the workgroup router:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod Menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating that it is opening the session to your console.
- Step 4** Verify that the first two serial interfaces are configured for HDLC by using the **show interfaces serial** command. The fourth line in the output should indicate your encapsulation type.
- Step 5** Verify the type of cable that is on your second serial interface (DCE or DTE) by using the **show controllers serial interface** command.
- Step 6** Label the diagram in the Exercise Preparation topic of this lab exercise to indicate which end of each cable is DTE and which end is DCE.
- Step 7** Enter global configuration mode.
- Step 8** Disable the IGRP routing protocol.

---

|             |                                                    |
|-------------|----------------------------------------------------|
| <b>Note</b> | Do not save configuration changes during this lab. |
|-------------|----------------------------------------------------|

---

- Step 9** Readdress your first serial interface by using the information provided in the Exercise Preparation topic of this lab exercise.
- Step 10** If you have the DCE side of the connection on your second serial interface, assign the **clock rate 64000**.
- Step 11** Configure your second serial interface with the proper IP address and encapsulation to connect to your neighbor pod. Use HDLC encapsulation if you found it was not configured for HDLC using the **show interfaces serial** command. Use the IP address in the table in the Exercise Preparation topic of this lab exercise.
- Step 12** Use the **no shutdown** command on your second serial interface.
- Step 13** Enable the EIGRP routing protocol. Use the EIGRP autonomous system number value in the table in the Exercise Preparation topic of this lab exercise.
- Step 14** Enter the network number for your 192.168.x.0 network in the EIGRP router process created in the step above.
- Step 15** Exit global configuration mode.
- Step 16** Use the appropriate commands to ensure that you have connectivity and can see your neighbor.
- Step 17** Proceed to Task 2.

## Task 2: Verify Routing with EIGRP

Now that you have EIGRP routing configured, you will verify the configuration and operation of the routing protocol. You will use two **show** commands that you have used in previous lab exercises.

Complete the following steps on the workgroup router:

- Step 1** Use the **show ip route** command to verify that the routes are learned from the EIGRP routing protocol. Your output should look similar to the following display:

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

Gateway of last resort is not set
```

```
D 172.16.0.0/16 [90/2809856] via 192.168.1.18, 00:05:24,
Serial0/1
 10.0.0.0/24 is subnetted, 1 subnets
C 10.2.2.0 is directly connected, Ethernet0/0
 192.168.1.0/28 is subnetted, 3 subnets
C 192.168.1.32 is directly connected, Serial0/0
D 192.168.1.48 [90/2681856] via 192.168.1.18, 00:05:25,
Serial0/1
C 192.168.1.16 is directly connected, Serial0/1
```

- Step 2** Use the **show ip protocols** command to verify that the EIGRP routing protocol is enabled and that EIGRP recognizes the autonomous groups that you assigned in the previous step. Your output should look similar to the following display:

```
wg_ro_z#show ip protocols
Routing Protocol is "eigrp 100"
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 EIGRP maximum hopcount 100
 EIGRP maximum metric variance 1
 Redistributing: eigrp 100
 Automatic network summarization is in effect
 Routing for Networks:
 192.168.1.0
 Routing Information Sources:
 Gateway Distance Last Update
 192.168.1.33 90 00:00:20
 192.168.1.18 90 00:00:20
 Distance: internal 90 external 170
wg_sw_z#
```

- Step 3** Proceed to Task 3.

## Task 3: Debug Routing with EIGRP

Now you will debug the EIGRP routing protocol. This will help you know what to look for when you need to troubleshoot EIGRP routing protocol issues.

Complete the following steps on the workgroup router:

- Step 1** Display the EIGRP neighbor events with the **debug eigrp neighbors** command.
- Step 2** Enter the interface configuration mode and **shutdown** your second serial interface.
- Step 3** Wait 10 seconds and then enter **no shutdown** on your serial interface. Your output should look similar to the following display:

```
wg_ro_z#debug eigrp neighbors
EIGRP Neighbors debugging is on
wg_ro_z#conf t
Enter configuration commands, one per line. End with CNTL/Z.
wg_ro_z(config)#interface serial 0/1
wg_ro_z(config-if)#shutdown
wg_ro_z(config-if)#
00:15:45: EIGRP: Neighbor 192.168.1.18 went down on Serial0/1
wg_ro_z(config-if)#
00:15:47: %LINK-5-CHANGED: Interface Serial0/1, changed state
to administratively down
00:15:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to down
wg_ro_z(config-if)#no shutdown
wg_ro_z(config-if)#
00:15:55: %LINK-3-UPDOWN: Interface Serial0/1, changed state
to up
wg_ro_z(config-if)#
00:15:55: EIGRP: Neighbor not yet found
wg_ro_z(config-if)#
00:15:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to up
wg_ro_z(config-if)#
00:15:57: EIGRP: Neighbor not yet found
00:15:57: EIGRP: New peer 192.168.1.18
wg_ro_z(config-if)#end
wg_ro_z#
00:16:02: %SYS-5-CONFIG_I: Configured from console by console
Turn off the display of EIGRP routing updates and all other
debugging.
```

- Step 4** Turn debugging off.
- Step 5** Verify that you can ping the core router loopback address (172.16.31.100) successfully from your router.
- Step 6** Disable EIGRP routing. After the Open Shortest Path First (OSPF) lab exercise, you will use IGRP in the remaining lab exercises.
- Step 7** Return to privileged EXEC mode and log out of your router.
- Step 8** Notify your instructor that you have completed the exercise.

## Exercise Verification

You have completed this exercise when you attain these results:

- You were able to learn the route to the core router with the EIGRP routing protocol.
- You were able to ping the core router loopback interface by using the dynamically learned route via the serial connection.



# Lab Exercise 3-4: Determining IP Routes with OSPF

Complete the lab exercise to practice what you learned in this module.

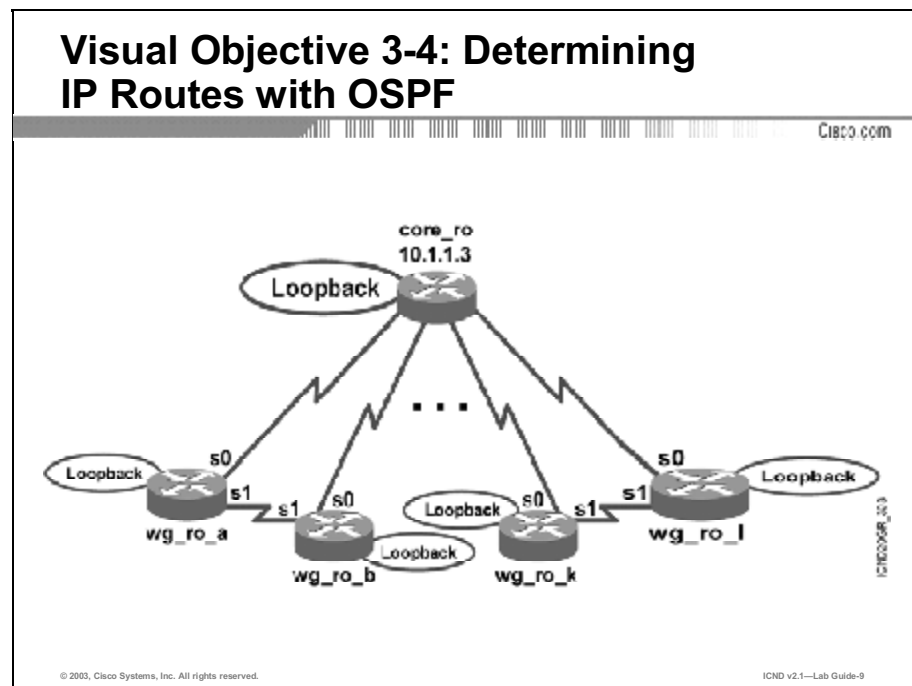
## Exercise Objective

Given a remote workgroup router and core office router with serial cables connecting both sites, you will enable the Open Shortest Path First (OSPF) routing protocol to dynamically learn about adjoining networks so that you can ping to the core router loopback interface via the serial connection. After completing this exercise, you will be able to meet these objectives:

- Enable routing with OSPF
- Monitor OSPF routing
- Debug routing with OSPF

## Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



## Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

## Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

| Command                                                                       | Description                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>bandwidth</b>                                                              | Configures the bandwidth on serial interfaces.                                                                                                                                                                                                             |
| <b>clock rate</b>                                                             | Configures the clock rate on serial interfaces.                                                                                                                                                                                                            |
| <b>debug ip ospf events</b>                                                   | Displays a summary of OSPF transaction information.                                                                                                                                                                                                        |
| <b>interface loopback</b>                                                     | Uses the interface global configuration command to configure an interface type and enter interface configuration mode.                                                                                                                                     |
| <b>network</b> <i>network-number wildcard-mask</i> <b>area</b> <i>area-id</i> | Starts up the routing protocol on all interfaces that the router has in the specified network, and specifies the number of bits significant for this network and the OSPF area with which it is associated.                                                |
| <b>ping</b> <i>ip-address</i>                                                 | Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The <b>ping</b> command also measures the amount of time it takes to receive the echo reply. |
| <b>router ospf</b> <i>router-process-id</i>                                   | Enables the OSPF routing protocol.                                                                                                                                                                                                                         |
| <b>show controllers</b> <i>type</i>                                           | Displays the controller state that is specific to the controller hardware.                                                                                                                                                                                 |
| <b>show interfaces</b> <i>type</i>                                            | Displays statistics for interfaces configured on the router.                                                                                                                                                                                               |
| <b>show ip ospf neighbor</b>                                                  | Determines the state of an OSPF neighbor.                                                                                                                                                                                                                  |
| <b>show ip protocols</b>                                                      | Displays values about routing protocols and routing protocol timer information associated with the router.                                                                                                                                                 |
| <b>show ip route</b>                                                          | Displays the IP routing table.                                                                                                                                                                                                                             |
| <b>shutdown/no shutdown</b>                                                   | Disables or enables an interface.                                                                                                                                                                                                                          |
| <b>undebug all</b>                                                            | Turns off all debugging displays.                                                                                                                                                                                                                          |

## Job Aids

There are no job aids for this lab exercise.

## Exercise Preparation

In this lab exercise, you will configure the OSPF routing protocol, the last of the four dynamic routing protocols you will configure in this course. Then you will verify the configuration and operation of OSPF. Finally, you will debug the routing protocol.

Before you complete this lab exercise, check with the instructor to make sure OSPF is configured on the core router.

The table lists the IP addresses that you will use in this lab exercise. Subnet masks are indicated with the */bits* to indicate the number of bits in the mask.

| Work group | Loopback0 on Workgroup Router (wg_ro_x) | Serial1 on Workgroup Router (wg_ro_x) | Serial0 on Workgroup Router (Example: wg_ro_a) | Core Router Serial Interface Address (core_ro) | Core Loopback Address | OSPF Process ID |
|------------|-----------------------------------------|---------------------------------------|------------------------------------------------|------------------------------------------------|-----------------------|-----------------|
| A          | 192.168.1.65/28                         | 192.168.1.17/28                       | 192.168.1.34/28                                | 192.168.1.33/28                                | 172.16.31.100         | 100             |
| B          | 192.168.1.81/28                         | 192.168.1.18/28                       | 192.168.1.50/28                                | 192.168.1.49/28                                | 172.16.31.100         | 100             |
| C          | 192.168.2.65/28                         | 192.168.2.17/28                       | 192.168.2.34/28                                | 192.168.2.33/28                                | 172.16.32.100         | 200             |
| D          | 192.168.2.81/28                         | 192.168.2.18/28                       | 192.168.2.50/28                                | 192.168.2.49/28                                | 172.16.32.100         | 200             |
| E          | 192.168.3.65/28                         | 192.168.3.17/28                       | 192.168.3.34/28                                | 192.168.3.33/28                                | 172.16.33.100         | 300             |
| F          | 192.168.3.81/28                         | 192.168.3.18/28                       | 192.168.3.50/28                                | 192.168.3.49/28                                | 172.16.33.100         | 300             |
| G          | 192.168.4.65/28                         | 192.168.4.17/28                       | 192.168.4.34/28                                | 192.168.4.33/28                                | 172.16.34.100         | 400             |
| H          | 192.168.4.81/28                         | 192.168.4.18/28                       | 192.168.4.50/28                                | 192.168.4.49/28                                | 172.16.34.100         | 400             |
| I          | 192.168.5.65/28                         | 192.168.5.17/28                       | 192.168.5.34/28                                | 192.168.5.33/28                                | 172.16.35.100         | 500             |
| J          | 192.168.5.81/28                         | 192.168.5.18/28                       | 192.168.5.50/28                                | 192.168.5.49/28                                | 172.16.35.100         | 500             |
| K          | 192.168.6.65/28                         | 192.168.6.17/28                       | 192.168.6.34/28                                | 192.168.6.33/28                                | 172.16.36.100         | 600             |
| L          | 192.168.6.81/28                         | 192.168.6.18/28                       | 192.168.6.50/28                                | 192.168.6.49/28                                | 172.16.36.100         | 600             |

## Task 1: Enable Routing with OSPF

The purpose of this task is to configure OSPF on the router. You will do this by assigning the routing process ID and identifying the networks that will participate in the OSPF routing process.

Complete the following steps on the workgroup router:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Enter global configuration mode.

---

|             |                                                                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Do not save configuration changes during this lab. You will use IGRP for the labs after this lab exercise, so do not save changes to NVRAM during this lab. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

- Step 5** Configure the loopback interface with the address indicated in the Exercise Preparation topic of this lab exercise.

What are two reasons that a loopback interface is useful?

- 
- Step 6** Verify that your second serial interface is configured to connect to your neighbor pod.
  - Step 7** Verify that you are using HDLC encapsulation and that the clock rate is 64000 on the appropriate side of the interface.
  - Step 8** Verify that the **bandwidth** command output matches the speed of your link. Both serial interfaces should be set to a bandwidth of 64 kbps.

---

|             |                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | If you did not complete the previous lab or your configuration has changed, enter the commands to establish connectivity to your partner pod via your second serial interface. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

- Step 9** Enable the OSPF routing protocol. Use the appropriate routing process ID as listed in the Exercise Preparation topic of this lab exercise.
- Step 10** Enable your loopback 0 interface and your two serial interfaces for OSPF. These interfaces should be in area 0. Use three network statements with a wildcard mask of 0.0.0.0. For example:  
  

```
network 10.1.1.1 0.0.0.0 area 0
network 10.2.2.1 0.0.0.0 area 0
network 10.3.3.1 0.0.0.0 area 0
```
- Step 11** Proceed to Task 2.

## Task 2: Monitor OSPF Routing

In this topic, you will verify the operation and configuration of the routing protocol. You will do this using two **show** commands.

Complete the following steps on the workgroup router:

- Step 1** Use the **show ip route** command to verify the routes learned from OSPF routing protocol. Your output should look similar to the following display:

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

Gateway of last resort is not set

 172.16.0.0/32 is subnetted, 1 subnets
O 172.16.31.100 [110/1563] via 192.168.1.33, 00:04:08,
Serial0/0
 10.0.0.0/24 is subnetted, 1 subnets
C 10.2.2.0 is directly connected, Ethernet0/0
 192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
C 192.168.1.64/28 is directly connected, Loopback0
O 192.168.1.81/32 [110/1563] via 192.168.1.18, 00:04:09,
Serial0/1
C 192.168.1.32/28 is directly connected, Serial0/0
O 192.168.1.48/28 [110/3124] via 192.168.1.18, 00:04:09,
Serial0/1
 [110/3124] via 192.168.1.33, 00:04:09,
Serial0/0
C 192.168.1.16/28 is directly connected, Serial0/1
wg_ro_z#
```

- Step 2** Use the **show ip protocols** command to verify that the OSPF routing protocol is enabled and that the routing process IDs you assigned in the previous step are recognized by OSPF. Your output should look similar to the following display:

```
wg_ro_z#show ip protocols
Routing Protocol is "ospf 100"
 Sending updates every 0 seconds
 Invalid after 0 seconds, hold down 0, flushed after 0
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: ospf 100
 Routing for Networks:
 192.168.1.17/32
 192.168.1.34/32
 192.168.1.65/32
 Routing Information Sources:
 Gateway Distance Last Update
 192.168.1.81 110 00:07:25
```

```

172.16.31.100 110 00:07:25
Distance: (default is 110)
wg_ro_z#

```

**Step 3** Use the **show ip ospf neighbor** command to display the neighbor status. Your output should look similar to the following display:

```

wg_ro_z#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address
Interface
172.16.36.100 1 FULL/ - 00:00:32 192.168.1.33
Serial0/0
192.168.1.81 1 FULL/ - 00:00:31 192.168.1.18
Serial0/1
wg_ro_z#

```

What is the neighbor state to the core and adjacent pod router?

---

What is the neighbor ID used by these routers?

---



---

**Note** You cannot see your neighbor until they complete Task 1 of this lab exercise.

---

**Step 4** Proceed to Task 3.

## Task 3: Debug Routing with OSPF

The purpose of this task is to acquaint you with the debug commands that will help you when you need to troubleshoot OSPF routing issues.

Complete the following steps on the workgroup router:

**Step 1** Display the OSPF HELLO messages sent to the router with the **debug ip ospf events** command. Your output should look similar to the following display

```

wg_ro_z#debug ip ospf events
OSPF events debugging is on
wg_ro_z#
11:12:37: OSPF: Rcv hello from 172.31.1.2 area 0 from Serial0
10.140.2.1
11:12:37: OSPF: End of hello processing
wg_ro_z#
11:12:47: OSPF: Rcv hello from 172.31.1.2 area 0 from Serial0
10.140.2.1
11:12:47: OSPF: End of hello processing
wg_ro_z#
11:12:57: OSPF: Rcv hello from 172.31.1.2 area 0 from Serial0
10.140.2.1
11:12:57: OSPF: End of hello processing
wg_ro_z#
11:13:07: OSPF: Rcv hello from 172.31.1.2 area 0 from Serial0
10.140.2.1
11:13:07: OSPF: End of hello processing

```

- Step 2** Turn debugging off. Your output should look similar to the following display
- ```
wg_ro_z#undebug all
All possible debugging has been turned off
wg_ro_z#
```
- Step 3** Ping the core router loopback address for your pod. Use the table in the Exercise Preparation topic for this lab exercise to determine the core router loopback address for your pod.
- Step 4** Disable OSPF routing. You will use IGRP in the remaining lab exercises.
- Step 5** Return to privileged EXEC mode.
- Step 6** Reload your router without saving the running configuration to revert your configuration back to the IGRP configuration. You will use the IGRP configuration for the remaining lab exercises.

Note	If you do not have your IGRP configuration saved in NVRAM, notify your instructor.

- Step 7** Verify that you can ping the core router (10.1.1.3).
- Step 8** Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You were able to learn the route to the core router with the OSPF routing protocol.
- You were able to ping the core router using the dynamically learned route via the serial connection.

Lab Exercise 4-1: Configuring IP Access Lists

Complete the lab exercise to practice what you learned in this module.

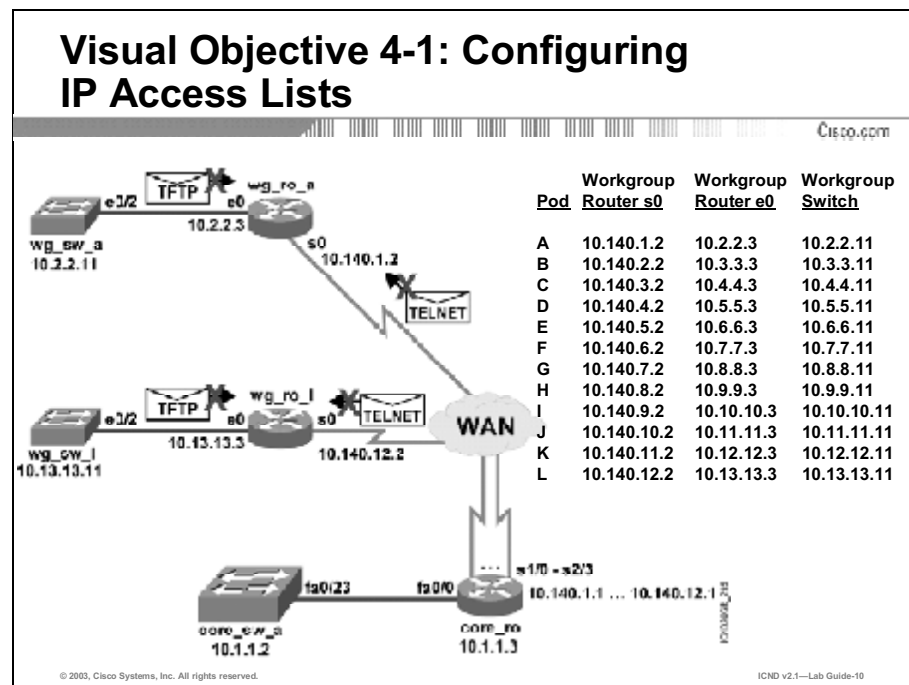
Exercise Objective

In this lab exercise, you will create an extended IP access list to block all Telnet traffic into your pod while allowing all other IP traffic, including pings. You will create an extended IP access list to block TFTP traffic from your workgroup switch to the core router while allowing all other traffic. After completing this exercise, you will be able to meet these objectives:

- Create an IP extended access list to block Telnet traffic
- Create an IP extended access list to block TFTP traffic from a core router to a workgroup switch
- Remove access lists from serial and Ethernet interfaces

Visual Objective

The figure illustrates the configuration that you will complete in this exercise.



Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

Command	Description
<code>access-list access-list-number {permit deny} {test conditions}</code>	Creates an extended IP access list.
<code>copy tftp://10.1.1.1/ filename nvram</code>	Copies the configuration from a TFTP server into NVRAM in a Catalyst 1900 switch.
<code>copy tftp://10.1.1.1/ filename startup-config</code>	Copies the configuration from a TFTP server into NVRAM in a Catalyst 2950 series switch.
<code>ip access-group access-list-number {in out}</code>	Enables an IP access list on an interface.
<code>ping ip-address</code>	Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The ping command also measures the amount of time it takes to receive the echo reply.
<code>show ip access-list</code>	Displays the contents of all IP access lists.
<code>show ip interface interface-type interface-number</code>	Displays the access lists applied on an interface.
<code>telnet ip-address</code>	Starts a terminal emulation program from a PC, router, or switch that permits you to access network devices remotely over the network.

Job Aids

There are no job aids for this lab exercise.

Exercise Preparation

Use the IP addresses in the table to complete this lab exercise.

Pod	Workgroup Router First Serial Interface	Core Router Serial Interface	Workgroup Switch	Workgroup Router Ethernet Interface
A	10.140.1.2	10.140.1.1	10.2.2.11	10.2.2.3
B	10.140.2.2	10.140.2.1	10.3.3.11	10.3.3.3
C	10.140.3.2	10.140.3.1	10.4.4.11	10.4.4.3
D	10.140.4.2	10.140.4.1	10.5.5.11	10.5.5.3
E	10.140.5.2	10.140.5.1	10.6.6.11	10.6.6.3
F	10.140.6.2	10.140.6.1	10.7.7.11	10.7.7.3
G	10.140.7.2	10.140.7.1	10.8.8.11	10.8.8.3
H	10.140.8.2	10.140.8.1	10.9.9.11	10.9.9.3
I	10.140.9.2	10.140.9.1	10.10.10.11	10.10.10.3
J	10.140.10.2	10.140.10.1	10.11.11.11	10.11.11.3
K	10.140.11.2	10.140.11.1	10.12.12.11	10.12.12.3
L	10.140.12.2	10.140.12.1	10.13.13.11	10.13.13.3

Task 1: Create an IP Extended Access List to Block Telnet Traffic into Your Pod

In this task, you will configure an extended IP access list to ensure that incoming Telnet traffic from outside of your pod is blocked. You will configure the access list, apply it to an interface, then verify it by having your instructor try to Telnet into your workgroup switch (which should fail) and ping the same device (which should succeed).

Complete the following steps on the workgroup router:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Enter global configuration mode.
- Step 5** Create an IP extended access list statement to only deny all Telnet traffic into your workgroup.
- Step 6** Apply the IP extended access list to your first serial interface.

Should the extended access list be applied as an input or output access list?

- Step 7** Exit global configuration mode.
- Step 8** Enter the **show ip access-list** command to display the content of your IP extended access list.
- Step 9** Enter the **show ip interface serial** interface command to verify that the access list is applied to the first serial interface.
- Step 10** Ask the instructor to try to Telnet from the core router to your workgroup switch. (All attempts to Telnet into your workgroup devices should fail.)
- Step 11** Ask the instructor to ping from the core router to your workgroup switch. (All other traffic into your workgroup devices except Telnet should work.)
- Step 12** Proceed to Task 2.

Task 2: Create an IP Extended Access List to Block TFTP Traffic from the Core Router to the Workgroup Switch

In this section, you will ensure that TFTP traffic from your workgroup switch to the TFTP server works. Then you will configure an extended IP access list that restricts inbound TFTP access from your workgroup switch. You will test the configuration by attempting to TFTP a configuration from the TFTP server to your workgroup switch (which should fail) and by pinging the TFTP server (which should succeed).

Note	Complete this task only if you have a TFTP server available. If a TFTP server is not available, proceed to Task 3 of this lab exercise.

Complete the following steps on the workgroup switch and workgroup router:

- Step 1** Test TFTP connectivity from your workgroup switch to the TFTP server by copying your workgroup switch configuration to the TFTP server (10.1.1.1). Name the file **wgswx.cfg**, where **x** is your pod letter. All TFTP traffic from your workgroup switch to the core router should work now.
- Step 2** At your workgroup router, enter global configuration mode.
- Step 3** Create an IP extended access list statement to only deny all TFTP traffic to your workgroup switch from the TFTP server.
- Step 4** Enter the interface configuration mode for your first Ethernet interface.
- Step 5** Apply the IP extended access list to your Ethernet interface.

Should you apply the access list as an input or output access list?

- Step 6** Exit interface configuration mode.
- Step 7** Exit global configuration mode.
- Step 8** Enter the **show ip access-list** command to display the content of your IP extended access list.

- Step 9** Enter the **show ip interface ethernet** interface command to verify that the access list is applied to the interface. Your output should look similar to the following display:

```
wg_ro_z#show ip interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Internet address is 10.13.13.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is 101
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  Web Cache Redirect is disabled
  BGP Policy Mapping is disabled
```

- Step 10** From your workgroup switch, try to TFTP the configuration (**wgswx.cfg**, where **x** is your pod letter) from the TFTP server (10.1.1.1) to your switch startup-config. All TFTP traffic from your workgroup switch should fail with the IP extended access list in place. You may have to wait for the TFTP to fail. The switch will retry the TFTP multiple times before displaying an error message.
- Step 11** Ping from your workgroup switch to the TFTP server (10.1.1.1). All traffic with the exception of TFTP traffic should work.
- Step 12** Proceed to Task 3.

Task 3: Remove the Access List from Serial and Ethernet Interfaces

The purpose of this task is to clean up after the lab so that the configuration changes you made here do not negatively impact the next lab. It is important to complete this task.

Complete the following steps on the workgroup router:

- Step 1** Enter interface configuration mode.
- Step 2** Remove all access lists from Ethernet and serial interfaces.
- Step 3** Enter global configuration mode.
- Step 4** Remove both access lists.
- Step 5** Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You were able to block Telnet traffic into your pod.
- You were able to block TFTP traffic from your workgroup switch.
- You were able to permit all other traffic.

In Task 3 at the end of the lab exercise, you were instructed to remove all access lists. Verify that you have removed both the **access-list** and **ip access-group** commands from the global and interface configurations.

Lab Exercise 4-2: Configuring Port Address Translation

Complete the lab exercise to practice what you learned in this module.

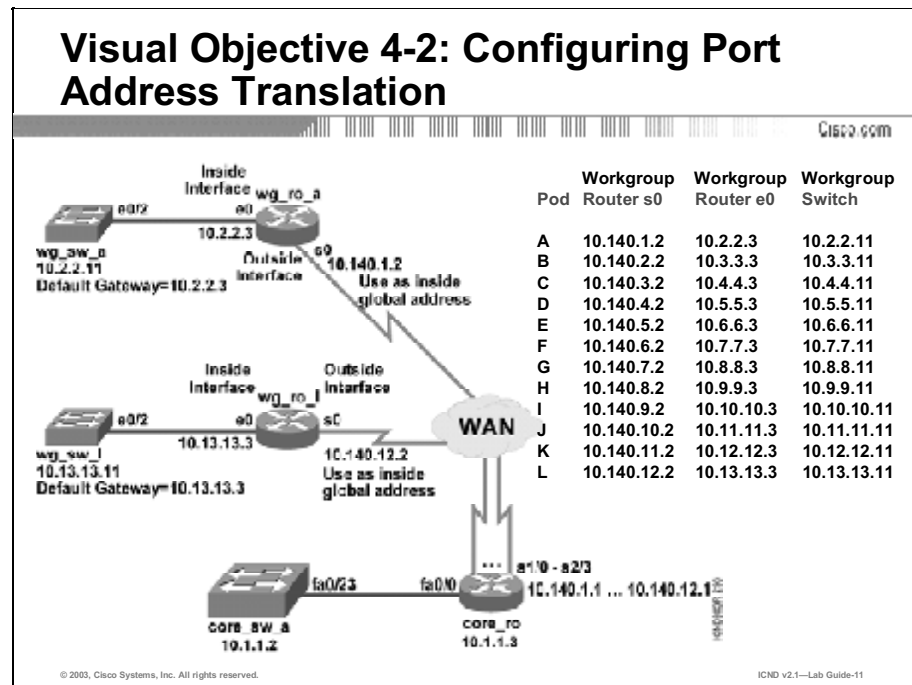
Exercise Objective

In this lab exercise, you will configure your workgroup router for port address translation (PAT). After completing this exercise, you will be able to meet these objectives:

- Configure PAT
- Verify PAT using **show** commands

Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

Command	Description
<code>ip nat inside</code>	Marks the interface as connected to the inside network.
<code>ip nat inside source list access-list-number interface interface overload</code>	Establishes dynamic source translation, specifying the access list.
<code>ip nat outside</code>	Marks the interface as connected to the outside network.
<code>show ip nat statistics</code>	Displays translation statistics.
<code>show ip nat translations</code>	Displays active translations.

Job Aids

There are no job aids for this lab exercise.

Exercise Preparation

The table lists the IP address information that you need to complete this lab exercise.

Workgroup	Workgroup Router Interface e0 IP Address (inside interface)	Workgroup Router Interface s0 IP Address (inside interface)
A	10.2.2.3	10.140.1.2
B	10.3.3.3	10.140.2.2
C	10.4.4.3	10.140.3.2
D	10.5.5.3	10.140.4.2
E	10.6.6.3	10.140.5.2
F	10.7.7.3	10.140.6.2
G	10.8.8.3	10.140.7.2
H	10.9.9.3	10.140.8.2
I	10.10.10.3	10.140.9.2
J	10.11.11.3	10.140.10.2
K	10.12.12.3	10.140.11.2
L	10.13.13.3	10.140.12.2

Task 1: Configure PAT

In this exercise, you will configure your router to provide a single address to the outside world for any inside address that needs to access the public network. First, you will verify that you have connectivity from your workgroup router to the core router. Then you will configure both inside and outside Network Address Translation (NAT) interfaces. Finally, you will configure an IP access list to permit certain hosts to use PAT.

Complete the following steps on the workgroup router to configure NAT:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup switch from the Pod menu and press **Return**.
- Step 4** Verify that you can ping the core router (10.1.1.3) from your workgroup switch. If the ping is not successful, troubleshoot the connectivity between your workgroup switch and the core router before proceeding with this lab exercise.
- Step 5** Disconnect your console session to the workgroup switch. Then select your workgroup router from the Pod menu and press **Return**.
- Step 6** To begin your NAT configuration, configure the first Ethernet interface on your workgroup router as the inside interface.
- Step 7** To continue the NAT configuration, configure the first serial interface of your workgroup router as the outside interface.
- Step 8** Configure a standard IP access list to permit any host on the 10.x.x.0/24 subnet to be translated by the PAT process.
- Step 9** Configure PAT using the first serial interface IP address as the inside global IP address.
- Step 10** Proceed to Task 2.

Task 2: Verify Port Address Translation Using show Commands

In this section, you will verify that port address translation is configured correctly.

Complete the following steps to verify port address translation:

Step 1 From your workgroup switch, verify that you can ping the core router (10.1.1.3) to trigger the PAT process on your workgroup router.

Step 2 From your workgroup router, enter the **show ip nat translations** command. Your output should look similar to the following display:

```
wg_ro_z#show ip nat translations
Pro  Inside global      Inside local      Outside local
Outside global
icmp 10.140.1.2:9392    10.2.2.11:9392    10.1.1.3:9392
10.1.1.3:9392
icmp 10.140.1.2:9393    10.2.2.11:9393    10.1.1.3:9393
10.1.1.3:9393
icmp 10.140.1.2:9394    10.2.2.11:9394    10.1.1.3:9394
10.1.1.3:9394
icmp 10.140.1.2:9395    10.2.2.11:9395    10.1.1.3:9395
10.1.1.3:9395
icmp 10.140.1.2:9396    10.2.2.11:9396    10.1.1.3:9396
10.1.1.3:9396
```

Step 3 Enter the **show ip nat statistics** command. Your output should look similar to the following display:

```
wg_ro_z#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:  Serial0
Inside interfaces:   Ethernet0
Hits: 5 Misses: 5
Expired translations: 5
Dynamic mappings:
-- Inside Source
Access list 1 interface s0 refcount 0
```

Step 4 Disable all PAT configurations on your workgroup router.

Step 5 Ping the core router (10.1.1.3) to verify that your configuration is working.

Step 6 Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You were able to ping from your workgroup switch to the core router.
- You saw the active port address translation sessions and statistics on your workgroup router.

At the end of this lab exercise, you were instructed to remove all NAT-related commands. Verify that this task has been done before considering this lab completed.

Lab Exercise 5-1: Configuring Serial Connections to WAN Service Providers

Complete the lab exercise to practice what you learned in this module.

Note This lab exercise is optional, depending on the amount of time you have available in your class.

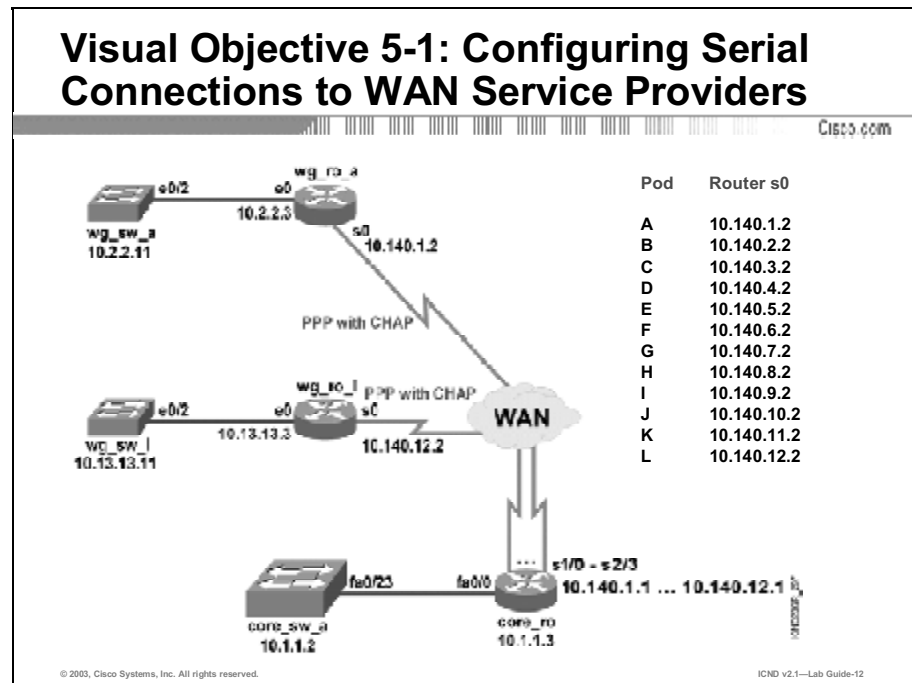
Exercise Objective

Given a workgroup and core with serial connections at each site, you will configure the workgroup router serial interface for PPP encapsulation with Challenge Handshake Authentication Protocol (CHAP) to complete a point-to-point connection to the core. After completing this exercise, you will be able to meet these objectives:

- Configure a PPP connection and enable CHAP authentication
- Verify PPP and CHAP operation

Visual Objective

The figure displays the configuration that you will complete in this lab exercise.



Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

Command	Description
<code>debug ppp authentication</code>	Debugs the PAP or CHAP authentication process.
<code>encapsulation ppp</code>	Enables PPP on an interface.
<code>ping ip-address</code>	Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The ping command also measures the amount of time it takes to receive the echo reply.
<code>ppp authentication chap</code>	Enables CHAP authentication on an interface.
<code>show interfaces</code>	Displays statistics for all interfaces configured on the router or access server.
<code>show running-config</code>	Displays the configuration information currently running on the router or the configuration for a specific interface.
<code>shutdown/no shutdown</code>	Disables or enables an interface.
<code>undebg all</code>	Turns off all debugging displays.
<code>username username</code> <code>password password</code>	Establishes a username-based authentication system.

Job Aids

There are no job aids for this lab exercise.

Exercise Preparation

Your instructor will have configured the core router to support this lab exercise.

The table lists the IP addresses for the serial connection required for this lab exercise.

Workgroup Pod	First Serial Interface on Workgroup Router	Core Router Serial Interface Address
A	10.140.1.2	10.140.1.1
B	10.140.2.2	10.140.2.1
C	10.140.3.2	10.140.3.1
D	10.140.4.2	10.140.4.1
E	10.140.5.2	10.140.5.1
F	10.140.6.2	10.140.6.1
G	10.140.7.2	10.140.7.1
H	10.140.8.2	10.140.8.1
I	10.140.9.2	10.140.9.1
J	10.140.10.2	10.140.10.1
K	10.140.11.2	10.140.11.1
L	10.140.12.2	10.140.12.1

Task 1: Configure a PPP Connection and Enable CHAP Authentication

This task gives you experience configuring the PPP on a serial interface and configuring CHAP as the authentication protocol.

Complete the following steps to configure PPP and enable CHAP on the workgroup router:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Enter privileged EXEC mode.
- Step 5** Enter the **show interfaces** command to verify that you have a working point-to-point connection. If the state of your interface is “line up, protocol down,” check to see if your instructor has already changed the serial encapsulation on core_ro to PPP.
- Step 6** Verify the IP address from the table in the Exercise Preparation section of this lab exercise.

What type of Layer 2 encapsulation is currently being used over the serial point-to-point connection? Why did you not have to manually configure a Layer 2 encapsulation on the interface?

-
- Step 7** While in the configuration mode for your first serial interface, administratively shut down this interface while completing the PPP configuration.
 - Step 8** Configure the first serial interface on your workgroup router for PPP encapsulation.
 - Step 9** While in interface configuration mode, enable CHAP authentication for the first serial interface on your workgroup router.
 - Step 10** In global configuration mode, create a username entry for the core router. Use the name **core_ro** and the password **cisco**. This lab exercise creates a two-way authentication scenario. For the core router to be authenticated by your local workgroup router, you must have a username entry in your local database.
 - Step 11** Verify that your host name is correctly configured on your router as wg_ro_x, where x is your pod letter.
 - Step 12** Leave your interface in **shutdown** mode.

- Step 13** Use the **show running-config** command to verify the configuration. Your output should look similar to the following display:

```
wg_ro_z#show running-config
!
hostname wg_sw_z
!
username core_ro password 0 cisco
!
interface Serial0
 ip address 10.140.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 no fair-queue
 ppp authentication chap
 shutdown
```

- Step 14** Proceed to Task 2.

Task 2: Verify PPP and CHAP Operation

This task gives you experience in verifying the operation of PPP and CHAP. As part of this task, you will use and become familiar with a helpful **debug** command.

Complete the following steps to verify PPP and CHAP operation on the workgroup router:

- Step 1** Enter privileged EXEC mode.
- Step 2** Enter the **debug ppp authentication** command to display the CHAP exchange sequence.
- Step 3** Enter the **no shutdown** command to enable your first serial interface.
- Step 4** Observe the CHAP exchange display. Your output should look similar to the following display:

```
wg_ro_z(config)#interface s0
wg_ro_z(config-if)#no shutdown
wg_ro_z(config-if)#
4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "wg_sw_z"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "core_ro"
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "wg_sw_z"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "core_ro"
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0, changed state to
up
wg_ro_z(config-if)#
```

Did your router pass the CHAP authentication? If not, check to make sure you did the following:

- Configured the appropriate interfaces with PPP encapsulation for the router
- Entered the correct username and password, in the correct case, on your router
- Enabled your interface on your router

- Step 5** When your authentication is successful, turn off **debug**.
- Step 6** Verify connectivity by pinging the core router serial interface and the Fast Ethernet core router interface at 10.1.1.3.
- Step 7** Use the **show interfaces** command to verify that the first serial interface on your router is configured for PPP encapsulation. Your output should look similar to the following display:

```
wg_ro_z#show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,
load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer
    Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
  abort
    38097 packets output, 2135697 bytes, 0 underruns
    0 output errors, 0 collisions, 6045 interface resets
    0 output buffer failures, 0 output buffers swapped out
    482 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

- Step 8** Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You pinged across the PPP connection.

Lab Exercise 6-1: Connecting to Frame Relay Services

Complete the lab exercise to practice what you learned in this module.

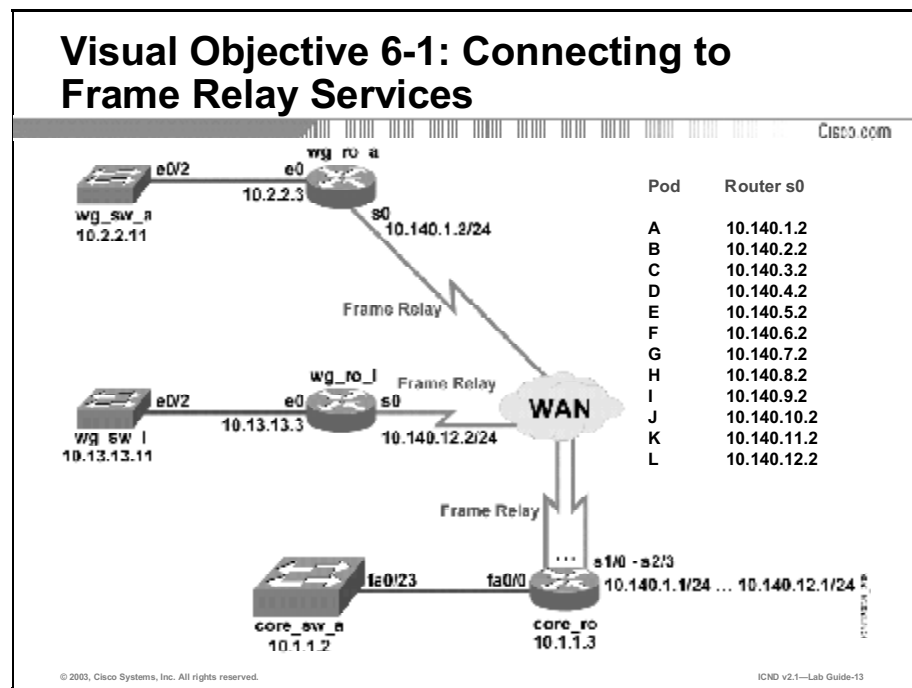
Exercise Objective

Given a remote workgroup router and a core router with serial connections to a packet-switched network, you will configure the workgroup router serial interface for Frame Relay encapsulation to complete a packet-switched connection to the core. After completing this exercise, you will be able to meet these objectives:

- Enable a Frame Relay connection
- Verify the Frame Relay connection
- Use the **debug frame-relay lmi** command to view LMI exchanges
- Configure and verify Frame Relay subinterfaces

Visual Objective

The figure illustrates the configuration that you will complete in this exercise.



Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

Command	Description
<code>debug frame relay lmi</code>	Displays debug information for Frame Relay LMI signaling.
<code>encapsulation frame-relay</code>	Enables Frame Relay encapsulation on an interface.
<code>frame-relay interface-dlci <i>dlci-number</i></code>	Specifies a DLCI ¹ identifier on a point-to-point subinterface.
<code>interface serial <i>number.subinterface-number</i> {multipoint point-to-point}</code>	Enters subinterface configuration mode and selects either a point-to-point or multipoint connection.
<code>ping <i>ip-address</i></code>	Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The ping command also measures the amount of time it takes to receive the echo reply.
<code>show frame-relay lmi</code>	Displays LMI information.
<code>show frame-relay map</code>	Displays Frame Relay route maps.
<code>show frame-relay pvc</code>	Displays PVC ² traffic statistics.
<code>show interfaces</code>	Displays interface information.
<code>show running-config</code>	Displays the active configuration.
<code>show running-config interface <i>type slot/port</i></code>	Displays the running configuration of the interface.

1 DLCI = data-link connection identifier

2 PVC = permanent virtual circuit

Job Aids

There are no job aids for this lab exercise.

Exercise Preparation

The table lists the IP addresses for the serial connection.

Workgroup	Serial 0 on Workgroup Router (wg_ro_x)	Core Router Serial Interface Address (core_ro)	Local DLCI Identifying PVC to Core
A	10.140.1.2	10.140.1.1	100
B	10.140.2.2	10.140.2.1	110
C	10.140.3.2	10.140.3.1	120
D	10.140.4.2	10.140.4.1	130
E	10.140.5.2	10.140.5.1	140
F	10.140.6.2	10.140.6.1	150
G	10.140.7.2	10.140.7.1	160
H	10.140.8.2	10.140.8.1	170
I	10.140.9.2	10.140.9.1	200
J	10.140.10.2	10.140.10.1	210
K	10.140.11.2	10.140.11.1	220
L	10.140.12.2	10.140.12.1	230

Task 1: Enable a Frame Relay Connection

For this task, you will configure your first serial interface to use Frame Relay encapsulation.

Complete the following steps on the core router to enable a Frame Relay connection:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Enter interface configuration mode for the first serial interface on the workgroup router and shut it down.
- Step 5** Enable Frame Relay on the interface. The LMI type will be determined using autosensing. Inverse Address Resolution Protocol (Inverse ARP) is used to map IP addresses to data-link connection identifiers (DLCIs).
- Step 6** Enable the interface.
- Step 7** Use the **show running-config** command for the serial 0/0 interface. Your output should look similar to the following display:

```
interface Serial 0
 ip address 10.140.1.2 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
```

- Step 8** Proceed to Task 2.

Task 2: Verify a Frame Relay Connection

For this task, you will verify the configuration using **show** commands and by pinging the core router.

Complete the following steps on the core router to verify the Frame Relay connection:

- Step 1** Verify that your first serial interface is in the up state with the **show interfaces serial x** command. Your output should look similar to the following display:

```
wg_ro_z#show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,
load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive set
(10 sec)
  LMI enq sent 19, LMI stat recvd 20, LMI upd recvd 0, DTE
LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface
broadcasts 5
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
```

```

Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 38756 packets input, 5695381 bytes, 0 no buffer
 Received 24172 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
 38777 packets output, 2164927 bytes, 0 underruns
 0 output errors, 0 collisions, 6069 interface resets
 0 output buffer failures, 0 output buffers swapped out
510 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

```

- Step 2** Verify the LMI type with the **show frame-relay lmi** command. Your output should look similar to the following display:

```

wg_ro_z#show frame-relay lmi
LMI Statistics for interface Serial0 (Frame Relay DTE) LMI
TYPE = CISCO
  Invalid Unnumbered info 0                Invalid Prot Disc 0
  Invalid dummy Call Ref 0                Invalid Msg Type 0
  Invalid Status Message 0                Invalid Lock Shift 0
  Invalid Information ID 0                Invalid Report IE Len
0
  Invalid Report Request 0                Invalid Keep IE Len 0
  Num Status Enq. Sent 18                Num Status msgs Rcvd
19
  Num Update Status Rcvd 0                Num Status Timeouts 0

```

- Step 3** Verify the PVC status with the **show frame-relay pvc** command. Your output should look similar to the following display:

```

wg_ro_z#show frame-relay pvc
PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE
= Serial0

  input pkts 28                output pkts 10                in bytes
8398
  out bytes 1198                dropped pkts 0                in FECN
pkts 0
  in BECN pkts 0                out FECN pkts 0                out BECN
pkts 0
  in DE pkts 0                out DE pkts 0
  out bcast pkts 10            out bcast bytes 1198
  pvc create time 00:03:46, last time pvc status changed
00:03:47

```

- Step 4** Verify that your Frame Relay map table lists a path to the core router by using the **show frame-relay map** command. Your output should look similar to the following display:

```

wg_ro_z#show frame-relay map
Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
              broadcast, status defined, active

```

- Step 5** Ping the serial interface of core router **core_ro** using the addresses provided in the Exercise Preparation section of this lab exercise.
- Step 6** Ping the core router at 10.1.1.3.
- Step 7** Proceed to Task 3.

Task 3: Use debug frame-relay lmi to View LMI Exchanges

LMI is used to convey information between a Frame Relay edge device, such as a router, and a Frame Relay switch. It is useful to see the LMI updates passed between the router and the switch when troubleshooting. In this task, you will configure the **debug frame-relay lmi** command and interpret the output.

Complete the following steps to view LMI exchanges on the workgroup router:

- Step 1** View the exchange of LMI status frames, including the Inverse ARP information, using the **debug frame-relay lmi** command. Your output should look similar to the following display:

```
wg_ro_z#debug frame lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
wg_ro_z#
1w2d: Serial0(out): StEnq, myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0(in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0(out): StEnq, myseq 141, yourseen 140, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0(in): Status, myseq 141
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 141, myseq 141
1w2d: Serial0(out): StEnq, myseq 142, yourseen 141, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 00 03 02 8E 8D
1w2d:
1w2d: Serial0(in): Status, myseq 142
1w2d: RT IE 1, length 1, type 0
1w2d: KA IE 3, length 2, yourseq 142, myseq 142
1w2d: PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
1w2d: Serial0(out): StEnq, myseq 143, yourseen 142, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8F 8E
```

- Step 2** Turn off all debugging.

- Step 3** Proceed to Task 4.

Task 4: Configure and Verify Frame Relay Subinterfaces

It is frequently necessary to use routing protocols to overcome split-horizon issues. One way to resolve split-horizon issues is to implement multiple logical interfaces on a single physical interface. These are called subinterfaces, and each may have its own IP address. In this task, you will configure a subinterface to be associated with a specific DLCI, Frame Relay Layer 2 addressing convention.

Complete the following steps from the workgroup router:

- Step 1** Prepare to configure a Frame Relay subinterface on the workgroup router by entering the global configuration mode.
- Step 2** Enter the interface configuration mode for your first serial interface.
- Step 3** Enter the **shutdown** command on the interface before using any other configuration commands.
- Step 4** Remove the IP address on the first serial interface.
- Step 5** Enter subinterface configuration mode for the first serial interface using the **interface s0.1 point-to-point** command. The subinterface should be point-to-point. The LMI type will be determined using autosensing.
- Step 6** Assign the IP address that was on the major interface to the subinterface. The addresses are listed in the table in the Exercise Preparation section of this lab exercise.
- Step 7** Configure the local DLCI identifying the PVC connection to the other side using the **frame-relay interface-dlci #** command, where # indicates the DLCI number. The DLCI numbers are listed in the Exercise Preparation section of this lab exercise.
- Step 8** Enter the **no shutdown** command on your first serial main interface.
- Step 9** Exit all configuration modes.
- Step 10** Verify your configuration with the **show running-config interface serial 0** and the **show running-config interface s0.1** commands. Your output should look similar to the following display:

```
wg_ro_z#show running-config interface serial 0
Building configuration...

Current configuration:
!
interface Serial0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 no fair-queue
end

wg_ro_z#show running-config interface serial 0.1
Building configuration...

Current configuration:
!
interface Serial0.1 point-to-point
 ip address 10.140.12.2 255.255.255.0
 no ip directed-broadcast
```

```
frame-relay interface-dlci 230
end
```

Step 11 Ping the core router at 10.1.1.3 to verify connectivity.

Step 12 Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You pinged across the Frame Relay connection.

Lab Exercise 7-1: Completing an ISDN BRI Call and Configuring DDR

Complete the lab exercise to practice what you learned in this module.

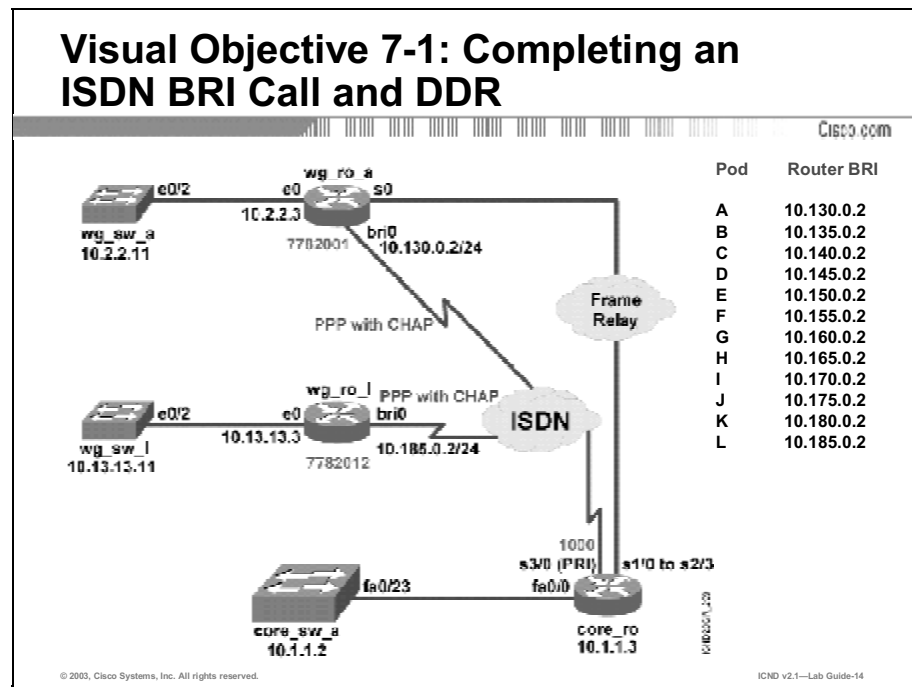
Exercise Objective

Given a workgroup and core site router with ISDN connections at each site, you will configure the workgroup router ISDN Basic Rate Interface (BRI) so that you can place a dial-on-demand routing (DDR) call to the core site. You will also configure the core router to receive the inbound call from the workgroup router. After completing this exercise, you will be able to meet these objectives:

- Configure a workgroup router ISDN BRI for DDR
- Configure the core router dialer interface

Visual Objective

The figure displays the configuration that you will complete in this exercise.



Required Resources

These are the resources and equipment required to complete this exercise:

- PC connected to an onsite lab, or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device if using a remote lab
- ICND pod assigned by your instructor

Command List

In this lab exercise, you will use the commands that are listed in the table. The commands are listed in alphabetical order so that you can easily locate the information you need. Refer to this list if you need configuration command assistance during the lab exercise.

Command	Description
debug dialer events	Displays debugging information about the packets received on a dialer interface.
debug isdn q931	Displays information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network.
dialer idle-timeout <i>seconds</i>	Specifies the idle time before the line is disconnected.
dialer map ip <i>next-hop-address name destination-router-name phone-number</i>	Specifies how to call a destination.
dialer pool <i>number</i>	Specifies the dialing pool to use for calls to this destination.
dialer pool-member <i>number</i>	Makes the interface a member of the dialing pool that the dialer interface will use; make sure the number arguments have the same value as with the dialer pool command. (Note: You will not enter this command, but you need to verify that it has been assigned to the proper interface so that your workgroup can connect to the core router.)
dialer remote-name <i>remote-router-name</i>	Configures the name of the remote router as passed for authentication.
dialer string <i>string</i>	Specifies the remote destination to call.
dialer-group <i>group-number</i>	Assigns a dialer group to an interface.
dialer-list <i>dialer-group protocol protocol-name {permit deny list access-list-number access-group}</i>	Specifies interesting traffic and associates it with a dialer group.
encapsulation ppp	Specifies PPP as the encapsulation type.
interface bri <i>number</i>	Enters interface configuration mode for the BRI.
interface dialer <i>interface-number</i>	Creates a virtual interface for use with a PRI to support multiple logical channels on a single physical interface.
ip address <i>ip-address mask</i>	Defines the IP address and subnet mask for the selected interface.
ip route <i>network mask next-hop-router-address</i>	Establishes static routes.
isdn switch-type basic-switch-type	Specifies a BRI switch type.
no router igrp <i>asn</i>	Disables IGRP for the specified autonomous system.
no shutdown	Enables an interface.
ping <i>ip-address</i>	Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The ping command also measures the amount of time it takes to receive the echo reply.
ppp authentication chap	Specifies CHAP authentication.

Command	Description
<code>show running-config</code>	Displays the current running configuration.
<code>username <i>username</i></code> <code>password <i>password</i></code>	Specifies the username and password of the authenticating device.

Job Aids

There are no job aids for this lab exercise.

Exercise Preparation

The table lists the IP addresses and phone numbers used in this lab exercise.

Workgroup	BRI0 Address on Workgroup Router	Workgroup BRI Phone Number	Core Router ISDN Interface	Core Router Phone Number
A	10.130.0.2	7782001	10.130.0.1	1000
B	10.135.0.2	7782002	10.135.0.1	1000
C	10.140.0.2	7782003	10.140.0.1	1000
D	10.145.0.2	7782004	10.145.0.1	1000
E	10.150.0.2	7782005	10.150.0.1	1000
F	10.155.0.2	7782006	10.155.0.1	1000
G	10.160.0.2	7782007	10.160.0.1	1000
H	10.165.0.2	7782008	10.165.0.1	1000
I	10.170.0.2	7782009	10.170.0.1	1000
J	10.175.0.2	7782010	10.175.0.1	1000
K	10.180.0.2	7782011	10.180.0.1	1000
L	10.185.0.2	7782012	10.185.0.1	1000

Task 1: Configure the Workgroup Router ISDN BRI for Dial-on-Demand Routing

This task requires you to configure the name and password for the device you will be calling (the core router), and define the encapsulation type and the authentication type you will use on the BRI. You will also need to define the kind of interesting traffic that will bring up the dial line, configure the idle timer to hang up after a period of inactivity, and map a static route to route traffic to the other end of your DDR link.

Complete the following steps to configure the workgroup router for ISDN BRI DDR:

- Step 1** From your PC, open a Telnet session to the terminal server. The Main menu appears.
- Step 2** Select your workgroup from the Main menu. The Pod menu appears.
- Step 3** Select your workgroup router from the Pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating it is opening the session to your console.
- Step 4** Enter global configuration mode.
- Step 5** Configure the username of the router to dial into and the password to use. Use **core_ro** as the name and **cisco** as the password.
- Step 6** Configure the dialer list to specify the type of interesting traffic that will generate a call to the remote router. In this lab exercise, all IP traffic will trigger the call. (Use dialer list 2 for this lab exercise.)
- Step 7** Configure the ISDN switch type specified by the ISDN service provider. In North America, the switch type is basic-5ess. If you are outside North America, ask your instructor for the switch type.
- Step 8** Enter interface configuration mode for the BRI.
- Step 9** Configure the BRI IP address, using a 24-bit subnet mask. Use the table in the Exercise Preparation section of this lab exercise to determine the correct IP address.
- Step 10** Configure PPP encapsulation on the BRI.
- Step 11** Enable CHAP authentication on the BRI.
- Step 12** Associate interesting traffic using the **dialer-group** command with the traffic identified on the dialer list you previously created.
- Step 13** Configure the timeout period to be 60 seconds. This is the time during which a lack of interesting traffic will allow the line to disconnect.
- Step 14** Map an IP destination address (Layer 3) with the destination phone number (Layer 2). Use the IP address of next hop router listed for each workgroup in the table in the Exercise Preparation section of this lab exercises. The destination router name and core router phone number are **core_ro** and **1000**, respectively.
- Step 15** Bring up the BRI0 interface.
- Step 16** From global configuration mode, disable all dynamic routing protocols.
- Step 17** Specify the static route in global configuration mode to reach the core office Ethernet network, 10.1.1.0 255.255.255.0, using the core router ISDN interface address given in the table as the next hop.
- Step 18** Exit global configuration mode.
- Step 19** Proceed to Task 2.

Task 2: Configure the Core Router Dialer Interface

In this section, you will examine the configuration of the Primary Rate Interface (PRI) controller and the serial interface associated with it. After recording the configurations for those two devices, you will create a logical interface for receiving your DDR calls, define the static route from the core router to your workgroup, and verify your configuration. Your access to the core router will be over the Frame Relay connection that you built in the previous lab exercise. Make sure that the connection is still active before attempting to configure the core router.

Complete the following steps to configure the core router to accept your dial-in call and route traffic to your workgroup:

- Step 1** Telnet to the core router using your configured Frame Relay connection. The destination address to use in your Telnet command is the IP address at the core router for that Frame Relay connection.
- Step 2** View the configuration of the PRI controller (either T1 or E1 interface) and the serial interface associated with this controller. Write down the configuration of each below.

Contoller T1 3/0

Serial interface 3/0:23

- Step 3** Enter global configuration mode on the core router.
- Step 4** Create a dialer interface using the **interface dialer x** command, where **x** is your pod letter (use Pod A=1 through Pod L=12). The dialer interface is necessary to receive an inbound call.
- Step 5** Configure the IP address and subnet mask on your dialer interface.
- Step 6** Configure the encapsulation type on the interface to PPP.
- Step 7** Configure CHAP authentication on the interface.
- Step 8** Configure the remote router name to wg_ro_x, where x is your pod letter.
- Step 9** Configure the dialer pool using the **dialer pool 4** command. The **dialer pool 4** command associates this logical interface with the PRI's serial interface. Refer to the configuration you copied from **serial interface 3/0:23** in Task 2 to see the relationship.
- Step 10** Use the **dialer idle-timeout 60** command to configure the dialer idle timeout.

- Step 11** Enter the **dialer string** command using the workgroup BRI phone number indicated in the table in the Exercise Preparation section of this lab exercise.
- Step 12** Configure the dialer-group to 1 to associate this interface with interesting traffic. Dialer-list 1 has already been configured on the core router as **dialer-list 1 protocol ip permit**.

Your finished configuration should resemble the following display:

```
interface Dialerx
 ip address 10.1--.0.1 255.255.255.0
 encapsulation ppp
 dialer remote-name wg_ro_x
 dialer idle-timeout 60
 dialer string 77820_ _
 dialer pool 4
 dialer-group 1
 ppp authentication chap
```

- Step 13** In global configuration mode, specify the static route to reach the Ethernet network in your workgroup. For example, for pod A, the static route configuration command is **ip route 10.2.2.0 255.255.255.0 10.130.0.2**.
- Step 14** Exit the global configuration mode.
- Step 15** Show the running configuration to verify the configuration of the logical interface for your workgroup and write the configuration below:

- Step 16** Ping the workgroup router and switch to test the configuration from the core router.
- Step 17** Terminate your Telnet session to return to your workgroup router EXEC prompt.
- Step 18** Proceed to Task 3.

Task 3: Verify ISDN Connectivity

This final task shows you how to use Cisco IOS commands to verify that your ISDN BRI DDR call is proceeding as expected. You will use **debug** commands to see the call setup and the DDR traffic.

Complete the following steps to see the call setup traffic and DDR traffic in the debug mode:

Step 1 Turn on debug isdn q931 and debug dialer events.

Step 2 Place a DDR call to the core router from the workgroup router. To place the call to the router, ping the core router IP address, 10.1.1.3. Watch the interesting traffic trigger the connection. Your output should look similar to the following display:

```
wg_ro_z#ping 10.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
28/30/32 ms
wg_ro_z#
01:19:37: BRI0/0 DDR: Dialing cause ip (s=10.130.0.2,
d=10.1.1.3)
01:19:37: BRI0/0 DDR: Attempting to dial 1000
01:19:37: ISDN BR0/0: TX -> SETUP pd = 8 callref = 0x15
01:19:37: Bearer Capability i = 0x8890
01:19:37: Channel ID i = 0x83
01:19:37: Keypad Facility i = '1000'
01:19:158913830912: ISDN BR0/0: RX <- CALL_PROC pd = 8
callref = 0x95
01:19:158913789952: Channel ID i = 0x89
01:19:158913830912: ISDN BR0/0: RX <- CONNECT pd = 8 callref
= 0x95
01:19:37: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to
up
01:19:37: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected
to 1000
01:19:37: ISDN BR0/0: TX -> CONNECT_ACK pd = 8 callref =
0x15
01:19:37: BRI0/0:1 DDR: dialer protocol up
01:19:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0/0:1, changed state
to up
wg_ro_z#
01:19:43: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected
to 1000 core_ro
wg_ro_z#
```

Step 3 Turn off all debugging.

Step 4 Notify your instructor that you have completed the exercise.

Exercise Verification

You have completed this exercise when you attain these results:

- You pinged the core router via the ISDN connection.

Lab Exercise Answer Key

Lab Exercise 1-1: Cisco Remote Lab Connection

There are no sample configurations for this lab exercise.

Lab Exercise 1-2: Configuring the Switch (Catalyst 1900 Series)

When you complete this lab exercise, your Catalyst 1900 series configuration will be similar to the following, with differences that are specific to your pod:

```
wg_ro_z#show running-config
Building configuration...
Current configuration:
!
mac-address-table permanent 00E0.1E5D.AE2F Ethernet 0/2
!
hostname "wg_sw_z"
!
address-violation disable
!
ip address 10.1.1.130 255.255.255.0
ip default-gateway 10.1.1.3
!
enable password level 15 "SANFRAN"
!
interface Ethernet 0/1
interface Ethernet 0/2
interface Ethernet 0/3
interface Ethernet 0/4
interface Ethernet 0/5
interface Ethernet 0/6
interface Ethernet 0/7
interface Ethernet 0/8
interface Ethernet 0/9
interface Ethernet 0/10
interface Ethernet 0/11
interface Ethernet 0/12
interface Ethernet 0/13
interface Ethernet 0/14
interface Ethernet 0/15
interface Ethernet 0/16
interface Ethernet 0/17
interface Ethernet 0/18
interface Ethernet 0/19
interface Ethernet 0/20
interface Ethernet 0/21
interface Ethernet 0/22
interface Ethernet 0/23
interface Ethernet 0/24
interface Ethernet 0/25
!
interface FastEthernet 0/26
interface FastEthernet 0/27
!
line console
end
```


Lab Exercise 1-2: Configuring the Switch (Catalyst 2950 Series)

When you complete this lab exercise, your Catalyst 2950 series configuration will be similar to the following, with differences that are specific to your pod:

```
wg_sw_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_sw_z
!
enable secret 5 $1$jIqt$0koMpj2DanDQB1S8AH67i.
enable password cisco
!
ip subnet-zero
!
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 VLAN1
 ip address 10.1.1.130 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 10.1.1.3
!
line con 0
 password cisco
 login
 transport input none
 stopbits 1
```

```

line vty 0 4
 password sanjose
 login
line vty 5 15
 password sanjose
 login
!
end

```

Workgroup Router Configuration

When you complete this lab exercise, your workgroup router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Ethernet0/0
 description First ethernet interface connects to wg_sw_z
 ip address 10.1.1.131 255.255.255.0
 no ip directed-broadcast
 no mop enabled
!
interface Serial0/0
 description First serial interface is configured as a DTE
interface
 bandwidth 64
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
interface BRI0/0
 no ip address
 no ip directed-broadcast
 shutdown
 isdn switch-type basic-5ess
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
!

```

```

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!
no scheduler allocate
end

```

Lab Exercise 2-1: Configuring a Switch for Extended Functionality (Catalyst 1900 Series)

When you complete this lab exercise, your Catalyst 1900 series configuration will be similar to the following, with differences that are specific to your pod:

```

wg_sw_z#show running-config
Building configuration...
Current configuration:
!
vtp domain "ICND"
vtp transparent
!
vlan 2 name "vlan2" sde 100002 state Operational mtu 1500
mac-address-table permanent 00E0.1E5D.AE2F Ethernet 0/2
!
hostname "wg_sw_z"
!
address-violation disable
!
ip address 10.1.1.130 255.255.255.0
ip default-gateway 10.1.1.3
!
enable password level 15 "SANFRAN"
!
interface Ethernet 0/1
!
interface Ethernet 0/2
  vlan-membership static 2
!
interface Ethernet 0/3
interface Ethernet 0/4
interface Ethernet 0/5
interface Ethernet 0/6
interface Ethernet 0/7
interface Ethernet 0/8
interface Ethernet 0/9
interface Ethernet 0/10
interface Ethernet 0/11
interface Ethernet 0/12
interface Ethernet 0/13

```

```

interface Ethernet 0/14
interface Ethernet 0/15
interface Ethernet 0/16
interface Ethernet 0/17
interface Ethernet 0/18
interface Ethernet 0/19
interface Ethernet 0/20
interface Ethernet 0/21
interface Ethernet 0/22
interface Ethernet 0/23
interface Ethernet 0/24
interface Ethernet 0/25
!
interface FastEthernet 0/26
!
    trunk On
interface FastEthernet 0/27
!
    trunk On
!
line console
end

```

Lab Exercise 2-1: Configuring a Switch for Extended Functionality (Catalyst 2950 Series)

When you complete this lab exercise, your Catalyst 2950 series configuration will be similar to the following, with differences that are specific to your pod:

```

wg_sw_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_sw_z
!
enable secret 5 $1$jIqt$Ok0Mpj2DanDQB1S8AH67i.
enable password cisco
!
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
    switchport access vlan 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
  switchport mode trunk
!
interface FastEthernet0/12
  switchport mode trunk
!
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 VLAN1
  ip address 10.1.1.130 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
!
ip default-gateway 10.1.1.3
!
line con 0
  password cisco
  login
  transport input none
  stopbits 1
line vty 0 4
  password sanjose
  login
line vty 5 15
  password sanjose
  login
!
end

```

Workgroup Router Configuration

When you complete this lab exercise, your workgroup router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero

```

```

isdn switch-type basic-5ess
!
interface Ethernet0/0
description First ethernet interface connects to wg_sw_z
ip address 10.14.14.12 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0/0
description First serial interface is configured as a DTE
interface
bandwidth 64
no ip address
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface BRI0/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface Serial0/1
no ip address
no ip directed-broadcast
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.3
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
exec-timeout 0 0
password cisco
login
transport input none
line aux 0
line vty 0 4
password sanjose
login
!
no scheduler allocate
end

```

Lab Exercise 3-1: Determining IP Routes with RIP

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!

```

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0/0
  description First ethernet interface connects to wg_sw_z
  ip address 10.14.14.3 255.255.255.0
  no ip directed-broadcast
  no mop enabled
!
interface Serial0/0
  description First serial interface is configured as a DTE
interface
  bandwidth 64
  ip address 10.140.13.2 255.255.255.0
  no ip directed-broadcast
  no ip mroute-cache
  no fair-queue
!
interface BRI0/0
  no ip address
  no ip directed-broadcast
  shutdown
  isdn switch-type basic-5ess
!
interface Serial0/1
  no ip address
  no ip directed-broadcast
  shutdown
!
router rip
  network 10.0.0.0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!

```

```
no scheduler allocate
end
```

Lab Exercise 3-2: Determining IP Routes with IGRP

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```
wg_ro_z#show running-config
Building configuration...

Current configuration:
!
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Ethernet0/0
description First ethernet interface connects to wg_sw_z
ip address 10.14.14.3 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0/0
description First serial interface is configured as a DTE
interface
bandwidth 64
ip address 10.140.13.2 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface BRI0/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface Serial0/1
no ip address
no ip directed-broadcast
shutdown
!
router igrp 200
network 10.0.0.0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
```



```

!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!
no scheduler allocate
end

```

Lab Exercise 3-3: Determining IP Routes with EIGRP

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Ethernet0/0
  description First ethernet interface connects to wg_sw_z
  ip address 10.14.14.3 255.255.255.0
  no ip directed-broadcast
  no mop enabled
!
interface Serial0/0
  description First serial interface is configured as a DTE
interface
  bandwidth 64
  ip address 192.168.7.34 255.255.255.240
  no ip directed-broadcast
  no ip mroute-cache
  no fair-queue
!
interface BRI0/0
  no ip address
  no ip directed-broadcast
  shutdown

```

```

    isdn switch-type basic-5ess
!
interface Serial0/1
 ip address 192.168.7.17 255.255.255.240
 no ip directed-broadcast
 clockrate 64000
!
router eigrp 100
 network 192.168.7.0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 password sanjose
 login
!
end

```

Lab Exercise 3-4: Determining IP Routes with OSPF

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Loopback0
 ip address 192.168.7.65 255.255.255.240
 no ip directed-broadcast
!
interface Ethernet0/0
 description First ethernet interface connects to wg_sw_z

```

```

ip address 10.14.14.3 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0/0
  description First serial interface is configured as a DTE
interface
  bandwidth 64
  ip address 192.168.7.34 255.255.255.240
  no ip directed-broadcast
  no ip mroute-cache
  no fair-queue
!
interface BRI0/0
  no ip address
  no ip directed-broadcast
  shutdown
  isdn switch-type basic-5ess
!
interface Serial0/1
  bandwidth 64
  ip address 192.168.7.17 255.255.255.240
  no ip directed-broadcast
  clockrate 64000
!
router ospf 100
  network 192.168.7.17 0.0.0.0 area 0
  network 192.168.7.34 0.0.0.0 area 0
  network 192.168.7.65 0.0.0.0 area 0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!
end

```

Lab Exercise 4-1: Configuring IP Access Lists

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!

```

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0/0
description First ethernet interface connects to wg_sw_z
ip address 10.14.14.3 255.255.255.0
ip access-group 102 in
no ip directed-broadcast
no mop enabled
!
interface Serial0/0
description First serial interface is configured as a DTE
interface
bandwidth 64
ip address 10.140.13.2 255.255.255.0
ip access-group 101 in
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface BRI0/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface Serial0/1
bandwidth 64
no ip address
no ip directed-broadcast
shutdown
clockrate 64000
!
router igrp 200
network 10.0.0.0
!
ip classless
!
access-list 101 deny tcp any any eq telnet
access-list 101 permit ip any any
access-list 102 deny udp any any eq tftp
access-list 102 permit ip any any
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0

```

```

exec-timeout 0 0
password cisco
login
transport input none
line aux 0
line vty 0 4
password sanjose
login
!
end

```

Lab Exercise 4-2: Configuring Port Address Translation

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Ethernet0/0
description First ethernet interface connects to wg_sw_z
ip address 10.14.14.3 255.255.255.0
no ip directed-broadcast
ip nat inside
no mop enabled
!
interface Serial0/0
description First serial interface is configured as a DTE
interface
bandwidth 64
ip address 10.140.13.2 255.255.255.0
no ip directed-broadcast
ip nat outside
no ip mroute-cache
no fair-queue
!
interface BRI0/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface Serial0/1
bandwidth 64
no ip address

```

```

no ip directed-broadcast
shutdown
clockrate 64000
!
router igrp 200
 network 10.0.0.0
!
ip nat inside source list 1 interface Serial0/0 overload
ip classless
!
access-list 1 permit 10.13.13.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 password sanjose
 login
!
end

```

Lab Exercise 5-1: Configuring Serial Connections to WAN Service Providers

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
username core_ro password 0 cisco
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0/0
 description First ethernet interface connects to wg_sw_z
 ip address 10.14.14.3 255.255.255.0
 no ip directed-broadcast
 no mop enabled
!
interface Serial0/0

```

```

        description First serial interface is configured as a DTE
interface
    bandwidth 64
    ip address 10.140.13.2 255.255.255.0
    no ip directed-broadcast
    encapsulation ppp
    no ip mroute-cache
    no fair-queue
    ppp authentication chap
!
interface BRI0/0
    no ip address
    no ip directed-broadcast
    shutdown
    isdn switch-type basic-5ess
!
interface Serial0/1
    bandwidth 64
    no ip address
    no ip directed-broadcast
    shutdown
    clockrate 64000
!
router igrp 200
    network 10.0.0.0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
    exec-timeout 0 0
    password cisco
    login
    transport input none
line aux 0
line vty 0 4
    password sanjose
    login
!
end

```

Lab Exercise 6-1: Connecting to Frame Relay Services

When you complete this lab exercise, your router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_z#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

```

```

!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
username core_ro password 0 cisco
ip subnet-zero
isdn switch-type basic-5ess
!
!
interface Ethernet0/0
description First ethernet interface connects to wg_sw_z
ip address 10.14.14.3 255.255.255.0
no ip directed-broadcast
no mop enabled
!
interface Serial0/0
description First serial interface is configured as a DTE
interface
bandwidth 64
no ip address
no ip directed-broadcast
encapsulation frame-relay
no ip mroute-cache
no fair-queue
!
interface Serial0/0.1 point-to-point
ip address 10.140.13.2 255.255.255.0
no ip directed-broadcast
frame-relay interface-dlci 100
!
interface BRI0/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface Serial0/1
bandwidth 64
no ip address
no ip directed-broadcast
shutdown
clockrate 64000
!
router igrp 200
network 10.0.0.0
!
ip classless
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
exec-timeout 0 0
password cisco
login

```



```

transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!
end

```

Lab Exercise 7-1: Completing an ISDN BRI Call and Configuring DDR

When you complete this lab exercise, your workgroup router configuration will be similar to the following, with differences that are specific to your pod:

```

wg_ro_x#show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg_ro_z
!
enable secret 5 $1$.7G/$U.jj9Px5In3n4s3K859Mz1
enable password cisco
!
username core_ro password 0 cisco
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0/0
  description First ethernet interface connects to wg_sw_z
  ip address 10.14.14.3 255.255.255.0
  no ip directed-broadcast
  no mop enabled
!
interface Serial0/0
  description First serial interface is configured as a DTE
interface
  bandwidth 64
  no ip address
  no ip directed-broadcast
  encapsulation frame-relay
  no ip mroute-cache
  no fair-queue
!
interface Serial0/0.1 point-to-point
  ip address 10.140.13.2 255.255.255.0
  no ip directed-broadcast
  frame-relay interface-dlci 100
!
interface BRI0/0
  ip address 10.190.0.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer idle-timeout 60
  dialer map ip 10.190.0.1 name core_ro 1000
  dialer-group 2
  isdn switch-type basic-5ess
  ppp authentication chap

```

```

!
interface Serial0/1
  bandwidth 64
  no ip address
  no ip directed-broadcast
  shutdown
  clockrate 64000
!
ip classless
ip route 10.1.1.0 255.255.255.0 10.190.0.1
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
dialer-list 2 protocol ip permit
!
banner motd ^C
authorized access only allowed to this router !!!
^C
!
line con 0
  exec-timeout 0 0
  password cisco
  login
  transport input none
line aux 0
line vty 0 4
  password sanjose
  login
!
end

```

Core Router Configuration

When you complete this lab exercise, your core router configuration will be similar to the following, with differences that are specific to your pod:

```

!ISDN LAB (STATIC ROUTE TO PODs)
!
hostname core_ro
!
enable password icndinstructor
!
username wg_ro_a password 0 cisco
username wg_ro_b password 0 cisco
username wg_ro_c password 0 cisco
username wg_ro_d password 0 cisco
username wg_ro_e password 0 cisco
username wg_ro_f password 0 cisco
username wg_ro_g password 0 cisco
username wg_ro_h password 0 cisco
username wg_ro_i password 0 cisco
username wg_ro_j password 0 cisco
username wg_ro_k password 0 cisco
username wg_ro_l password 0 cisco
!
isdn switch-type primary-5ess
!
controller T1 3/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-2

```

```

    no shut
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
no shut
!
interface Serial3/0:23
description -- pri channels config
encapsulation ppp
ppp auth chap
dialer pool-member 4
isdn switch-type primary-5ess
no shut
!
!
interface Dialer1
ip address 10.130.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_a
dialer idle-timeout 60
dialer string 7782001
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer2
ip address 10.135.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_b
dialer idle-timeout 60
dialer string 7782002
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer3
ip address 10.140.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_c
dialer idle-timeout 60
dialer string 7782003
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer4
ip address 10.145.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_d
dialer idle-timeout 60
dialer string 7782004
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer5
ip address 10.150.0.1 255.255.255.0

```

```

no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_e
dialer idle-timeout 60
dialer string 7782005
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer6
ip address 10.155.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_f
dialer idle-timeout 60
dialer string 7782006
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer7
ip address 10.160.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_g
dialer idle-timeout 60
dialer string 7782007
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer8
ip address 10.165.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_h
dialer idle-timeout 60
dialer string 7782008
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer9
ip address 10.170.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_i
dialer idle-timeout 60
dialer string 7782009
dialer pool 4
dialer-group 1
ppp authentication chap
!
interface Dialer10
ip address 10.175.0.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer remote-name wg_ro_j
dialer idle-timeout 60
dialer string 7782010
dialer pool 4

```

```

dialer-group 1
ppp authentication chap
!
interface Dialer11
 ip address 10.180.0.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer remote-name wg_ro_k
 dialer idle-timeout 60
 dialer string 7782011
 dialer pool 4
 dialer-group 1
 ppp authentication chap
!
interface Dialer12
 ip address 10.185.0.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer remote-name wg_ro_l
 dialer idle-timeout 60
 dialer string 7782012
 dialer pool 4
 dialer-group 1
 ppp authentication chap
!
interface Dialer13
 ip address 10.190.0.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer remote-name wg_ro_z
 dialer idle-timeout 60
 dialer string 7782013
 dialer pool 4
 dialer-group 1
 ppp authentication chap
!
ip route 10.2.2.0 255.255.255.0 dialer1
!
ip route 10.3.3.0 255.255.255.0 dialer2
!
ip route 10.4.4.0 255.255.255.0 dialer3
!
ip route 10.5.5.0 255.255.255.0 dialer4
!
ip route 10.6.6.0 255.255.255.0 dialer5
!
ip route 10.7.7.0 255.255.255.0 dialer6
!
ip route 10.8.8.0 255.255.255.0 dialer7
!
ip route 10.9.9.0 255.255.255.0 dialer8
!
ip route 10.10.10.0 255.255.255.0 dialer9
!
ip route 10.11.11.0 255.255.255.0 dialer10
!
ip route 10.12.12.0 255.255.255.0 dialer11
!
ip route 10.13.13.0 255.255.255.0 dialer12
!
ip route 10.14.14.0 255.255.255.0 dialer13

```

```
!  
!  
no router rip  
!  
no router igrp 200  
!  
dialer-list 1 protocol ip permit  
!  
end
```