

BSCI

Building Scalable Cisco Internetworks

Version 2.1

Student Guide

Copyright © 2004, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece
Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania
Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland
Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

 Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, iQ logo, the iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

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

Table of Contents

Volume 1

<u>Course Introduction</u>	1
Overview	1
Outline	1
Course Objectives	2
Cisco Certifications	5
Learner Skills and Knowledge	6
Learner Responsibilities	8
General Administration	9
Course Flow Diagram	10
Icons and Symbols	11
Learner Introductions	12
<u>Advanced IP Addressing</u>	1-1
Overview	1-1
Module Objectives	1-2
Module Outline	1-2
<u>Purpose of Address Planning</u>	1-3
Overview	1-3
Relevance	1-3
Objectives	1-3
Learner Skills and Knowledge	1-4
Outline	1-4
Scalable Network Design	1-5
Benefits of Good Network Design	1-11
Benefits of an Optimized IP Addressing Plan	1-15
Example	1-17
Update Size	1-18
Unsummarized Internetwork Topology Changes	1-18
Summarized Network Topology Changes	1-19
Summary	1-20
Quiz	1-21
Quiz Answer Key	1-22
<u>Hierarchical Addressing Using Variable-Length Subnet Masks</u>	1-23
Overview	1-23
Relevance	1-23
Objectives	1-23
Learner Skills and Knowledge	1-24
Outline	1-24
Prefix Length and Network Mask	1-25
Example	1-26
Implementing VLSM in a Scalable Network	1-28
Example	1-30
Calculating VLSM	1-31
Example	1-37
Summary	1-38
Quiz	1-39
Quiz Answer Key	1-40
<u>Route Summarization and Classless Interdomain Routing</u>	1-41
Overview	1-41
Relevance	1-41
Objectives	1-41
Learner Skills and Knowledge	1-42
Outline	1-42

Route Summarization	1-43
Example	1-44
Calculating Route Summarization	1-45
Example	1-47
Classless Interdomain Routing	1-48
Example	1-50
Summary	1-51
Quiz	1-52
Quiz Answer Key	1-53
Understanding IP Version 6	1-55
Overview	1-55
Relevance	1-55
Objectives	1-55
Learner Skills and Knowledge	1-55
Outline	1-56
Benefits of IP Version 6	1-57
IPv6 Addressing	1-58
IPv6 Frame Format	1-65
IPv6-to-IPv4 Interoperability	1-71
Summary	1-77
Quiz	1-78
Quiz Answer Key	1-80
Network Address Translation	1-81
Overview	1-81
Relevance	1-81
Objectives	1-81
Learner Skills and Knowledge	1-82
Outline	1-82
Configuring IP NAT with Access Lists	1-83
Example	1-86
Defining the Route Map Tool for NAT	1-87
Using Basic route-map Commands	1-89
Configuring IP NAT with Route Maps	1-90
Summary	1-92
Next Steps	1-92
Quiz	1-93
Quiz Answer Key	1-94
Lesson Assessments	1-95
Overview	1-95
Outline	1-95
Quiz 1-1: Purpose of Address Planning	1-96
Objectives	1-96
Quiz	1-96
Quiz 1-2: Hierarchical Addressing Using Variable-Length Subnet Masks	1-97
Objectives	1-97
Quiz	1-97
Scoring	1-97
Quiz 1-3: Route Summarization and Classless Interdomain Routing	1-98
Objectives	1-98
Task 1	1-98
Task 2	1-99
Scoring	1-99
Quiz 1-4: Understanding IP version 6	1-100
Objectives	1-100
Quiz	1-100

Scoring	1-102
Lesson Assessment Answer Key	1-103
<u>Routing Principles</u>	2-1
Overview	2-1
Module Objectives	2-1
Module Outline	2-2
<u>IP Routing Overview</u>	2-3
Overview	2-3
Relevance	2-3
Objectives	2-3
Learner Skills and Knowledge	2-3
Outline	2-4
Principles of Static Routing	2-5
Example	2-7
Configuring a Static Default Route	2-8
Example	2-8
Principles of Dynamic Routing	2-9
Example	2-11
Principles of On-Demand Routing	2-12
Configuring ODR	2-14
Example	2-15
Summary	2-16
Quiz	2-17
Quiz Answer Key	2-19
<u>Characteristics of Routing Protocols</u>	2-21
Overview	2-21
Relevance	2-21
Objectives	2-21
Learner Skills and Knowledge	2-22
Outline	2-22
Classful Routing Protocol Concepts	2-23
Automatic Network Boundary Summarization in a Classful Routing Protocol	2-25
Example	2-26
Examining a Classful Routing Table	2-28
Classless Routing Protocol Concepts	2-30
Example	2-31
Automatic Network Boundary Summarization Using RIPv2 and EIGRP	2-32
Example	2-32
The auto-summary Command for RIPv2 and EIGRP	2-34
Example	2-35
Characteristics of RIPv1	2-36
Characteristics and Configuration of RIPv2	2-37
Summary	2-42
Quiz	2-43
Quiz Answer Key	2-45
<u>IP Routing Protocol Comparison</u>	2-47
Overview	2-47
Relevance	2-47
Objectives	2-47
Learner Skills and Knowledge	2-47
Outline	2-48
Administrative Distance	2-49
Example	2-50
Floating Static Routes	2-51
Example	2-52

Criteria for Inserting Routes in the IP Routing Table	2-53
Comparing Routing Protocol Charts	2-55
Summary	2-59
Next Steps	2-59
Quiz	2-60
Quiz Answer Key	2-61
Lesson Assessments	2-63
Overview	2-63
Outline	2-63
Quiz 2-1: IP Routing Overview	2-64
Objectives	2-64
Quiz	2-64
Scoring	2-65
Quiz 2-2: Characteristics of Routing Protocols	2-66
Objectives	2-66
Quiz	2-66
Scoring	2-69
Quiz 2-3: IP Routing Protocol Comparison	2-70
Objectives	2-70
Quiz	2-70
Scoring	2-71
Lesson Assessment Answer Key	2-72
Configuring EIGRP	3-1
Overview	3-1
Module Objectives	3-2
Module Outline	3-2
EIGRP Overview	3-3
Overview	3-3
Relevance	3-3
Objectives	3-3
Learner Skills and Knowledge	3-3
Outline	3-4
Introduction	3-5
EIGRP Databases	3-7
Example	3-10
EIGRP Metrics Calculation	3-11
Example	3-15
Summary	3-17
Quiz	3-18
Quiz Answer Key	3-19
EIGRP Operations	3-21
Overview	3-21
Relevance	3-21
Objectives	3-21
Learner Skills and Knowledge	3-22
Outline	3-22
EIGRP Packets	3-23
Establishing Neighbors	3-27
EIGRP Reliability, Transmission Policy, and Transport Mechanism	3-29
Example	3-32
Initial Route Discovery in EIGRP	3-33
Verifying EIGRP Connectivity Using debug Commands	3-35
Summary	3-40
Quiz	3-41

Quiz Answer Key	3-43
EIGRP DUAL	3-45
Overview	3-45
Relevance	3-45
Objectives	3-45
Learner Skills and Knowledge	3-46
Outline	3-46
Selection of a Successor by DUAL	3-47
Example	3-48
Selection of a Feasible Successor by DUAL	3-50
Example	3-51
Selection When No Feasible Successor Is Available	3-52
EIGRP Query Process	3-53
Summary	3-60
Quiz	3-61
Quiz Answer Key	3-62
Configuring and Verifying EIGRP	3-63
Overview	3-63
Relevance	3-63
Objectives	3-63
Learner Skills and Knowledge	3-63
Outline	3-64
Configuring EIGRP	3-65
Example	3-67
Configuring Default Route Using the <code>default-network</code> Command	3-70
Verifying EIGRP Using <code>show</code> Commands	3-72
Summary	3-78
Next Steps	3-78
Quiz	3-79
Quiz Answer Key	3-80
Advanced EIGRP Configuration Options	3-81
Overview	3-81
Relevance	3-81
Objectives	3-81
Learner Skills and Knowledge	3-81
Outline	3-82
EIGRP Manual Route Summarization	3-83
Example	3-86
Understanding EIGRP Load Balancing	3-87
Load Balancing Across Unequal-Cost Paths Using Variance	3-88
Example	3-89
EIGRP Bandwidth Utilization	3-91
Example	3-94
Summary	3-96
Quiz	3-97
Quiz Answer Key	3-98
EIGRP in a Scalable Network	3-99
Overview	3-99
Relevance	3-99
Objectives	3-99
Learner Skills and Knowledge	3-99
Outline	3-100
How EIGRP Responds to a Query	3-101
Example	3-103
Scalability Issues and Solutions	3-107

LIMITING THE EIGRP QUERY RANGE	3-108
Example	3-111
LIMITING THE EIGRP QUERY RANGE USING THE STUB OPTION	3-113
Example	3-116
SCALABILITY RULES FOR IMPLEMENTING EIGRP	3-118
Summary	3-120
Quiz	3-121
Quiz Answer Key	3-122
Lesson Assessments	3-123
Overview	3-123
Outline	3-123
Quiz 3-1: EIGRP Overview	3-124
Objectives	3-124
Quiz	3-124
Scoring	3-125
Quiz 3-2: EIGRP Operations	3-126
Objectives	3-126
Quiz	3-126
Scoring	3-127
Quiz 3-3: EIGRP DUAL	3-128
Objectives	3-128
Quiz	3-128
Scoring	3-128
Quiz 3-4: Configuring and Verifying EIGRP	3-129
Objectives	3-129
Quiz	3-129
Scoring	3-129
Quiz 3-5: Advanced EIGRP Configuration Options	3-130
Objectives	3-130
Quiz	3-130
Scoring	3-130
Quiz 3-6: EIGRP in a Scalable Network	3-131
Objectives	3-131
Quiz	3-131
Scoring	3-131
Lesson Assessment Answer Key	3-132

Table of Contents

Volume 2

<u>Configuring OSPF</u>	4-1
Overview	4-1
Module Objectives	4-1
Module Outline	4-2
<u>OSPF Protocol Overview</u>	4-3
Overview	4-3
Relevance	4-3
Objectives	4-3
Learner Skills and Knowledge	4-3
Outline	4-4
Link-State Routing Protocols	4-5
Example	4-7
Defining an OSPF Area	4-8
Defining OSPF Adjacencies	4-11
OSPF Calculation	4-14
Summary	4-17
Quiz	4-18
Quiz Answer Key	4-20
<u>OSPF Packet Types</u>	4-21
Overview	4-21
Relevance	4-21
Objectives	4-21
Learner Skills and Knowledge	4-21
Outline	4-22
Types of OSPF Packets	4-23
OSPF Neighbor Adjacency Establishment	4-25
Exchange Process and OSPF Neighbor Adjacency States	4-27
OSPF Link-State Sequence Numbers	4-33
The debug ip ospf packet Command	4-35
Summary	4-37
Quiz	4-38
Quiz Answer Key	4-40
<u>Configuring Basic OSPF</u>	4-41
Overview	4-41
Relevance	4-41
Objectives	4-41
Learner Skills and Knowledge	4-41
Outline	4-42
Configuring Basic Single-Area OSPF	4-43
Manipulating the OSPF Router ID	4-51
Summary	4-55
Quiz	4-56
Quiz Answer Key	4-57
<u>OSPF Network Types</u>	4-59
Overview	4-59
Relevance	4-59
Objectives	4-59
Learner Skills and Knowledge	4-60
Outline	4-60
Adjacency Behavior for a Point-to-Point Link	4-61
Adjacency Behavior for a Broadcast Network	4-62
Adjacency Behavior for an NBMA Network	4-67

OSPF Commands for NBMA Network Frame Relay	4-69
Example	4-72
Common OSPF Configurations for Frame Relay	4-73
The debug ip ospf adj Command	4-86
Summary	4-88
Next Steps	4-88
Quiz	4-89
Quiz Answer Key	4-91
Types of OSPF Routers and Link-State Advertisements	4-93
Overview	4-93
Relevance	4-93
Objectives	4-93
Learner Skills and Knowledge	4-93
Outline	4-94
Types of OSPF Routers	4-95
OSPF LSA Types	4-98
Type 1	4-98
Type 2	4-98
Types 3 and 4	4-99
Type 5	4-99
Type 6	4-99
Type 7	4-99
Type 8	4-99
Types 9, 10, and 11	4-99
Interpreting the OSPF LSDB and Routing Table	4-105
Summary	4-110
Quiz	4-111
Quiz Answer Key	4-113
OSPF Route Summarization Techniques	4-115
Overview	4-115
Relevance	4-115
Objectives	4-115
Learner Skills and Knowledge	4-116
Outline	4-116
OSPF Route Summarization Concepts	4-117
Example	4-119
OSPF Route Summarization Commands	4-120
Example	4-123
Creating a Default Route in OSPF	4-124
The default-information originate Command	4-125
Example	4-127
Summary	4-128
Quiz	4-129
Quiz Answer Key	4-131
OSPF Special Area Types	4-133
Overview	4-133
Relevance	4-133
Objectives	4-133
Learner Skills and Knowledge	4-133
Outline	4-134
Types of OSPF Areas	4-135
Stub Areas	4-137
Totally Stubby Areas	4-140
Not-So-Stubby Areas	4-145
Summary	4-149

Next Steps	4-149
Quiz	4-150
Quiz Answer Key	4-152
OSPF Virtual Links	4-153
Overview	4-153
Relevance	4-153
Objectives	4-153
Learner Skills and Knowledge	4-153
Outline	4-154
Defining an OSPF Virtual Link	4-155
Configuring OSPF Virtual Links	4-157
Verifying OSPF Virtual Links Operation	4-162
Summary	4-164
Next Steps	4-164
Quiz	4-165
Quiz Answer Key	4-166
Lesson Assessments	4-167
Overview	4-167
Outline	4-167
Quiz 4-1: OSPF Protocol Overview	4-168
Objectives	4-168
Quiz	4-168
Scoring	4-169
Quiz 4-2: OSPF Packet Types	4-170
Objectives	4-170
Quiz	4-170
Scoring	4-171
Quiz 4-3: Configuring Basic OSPF	4-172
Objectives	4-172
Quiz	4-172
Scoring	4-173
Quiz 4-4: OSPF Network Types	4-174
Objectives	4-174
Quiz	4-174
Scoring	4-175
Quiz 4-5: Types of OSPF Routers and LSAs	4-176
Objectives	4-176
Quiz	4-176
Scoring	4-177
Quiz 4-6: OSPF Route Summarization Techniques	4-178
Objectives	4-178
Quiz	4-178
Scoring	4-179
Quiz 4-7: OSPF Special Area Types	4-180
Objectives	4-180
Quiz	4-180
Scoring	4-181
Quiz 4-8: OSPF Virtual Links	4-182
Objectives	4-182
Quiz	4-182
Scoring	4-183
Lesson Assessment Answer Key	4-184

<i>Configuring the IS-IS Protocol</i>	5-1
Overview	5-1
Module Objectives	5-2
Module Outline	5-2
<i>Overview of IS-IS Routing and CLNS</i>	5-3
Overview	5-3
Relevance	5-3
Objectives	5-3
Learner Skills and Knowledge	5-3
Outline	5-4
IS-IS Routing	5-5
Integrated IS-IS	5-6
ES-IS Protocol Operations	5-11
OSI Routing Levels	5-12
IS-IS Level 0 Routing	5-12
IS-IS Level 1 Routing	5-12
IS-IS Level 2 Routing	5-13
IS-IS Level 3 Routing	5-13
Summary	5-13
Comparing IS-IS and OSPF	5-14
Summary	5-21
References	5-21
Quiz	5-22
Quiz Answer Key	5-24
<i>Understanding CLNS Addressing</i>	5-25
Overview	5-25
Relevance	5-25
Objectives	5-25
Learner Skills and Knowledge	5-25
Outline	5-26
NSAP Addresses	5-27
NET Addresses	5-32
Summary	5-34
References	5-34
Quiz	5-35
Quiz Answer Key	5-36
<i>Basic Operations of IS-IS in a CLNS Environment</i>	5-37
Overview	5-37
Relevance	5-37
Objectives	5-37
Learner Skills and Knowledge	5-38
Outline	5-38
Intra-Area and Interarea Addressing and Routing	5-39
Example	5-41
IS-IS Routing Levels	5-42
IS-IS Protocol Data Units	5-45
Example	5-46
Link-State Packets	5-47
Topologies	5-51
Broadcast Networks	5-52
Point-to-Point Networks	5-55
Level 1 and Level 2 LSP	5-55
Level 1 and Level 2 IIH	5-55
Link-State Database Synchronization	5-57

Example	5-60
Summary	5-64
Quiz	5-65
Quiz Answer Key	5-68
Basic Operations of Integrated IS-IS in an IP and CLNS Environment	5-69
Overview	5-69
Relevance	5-69
Objectives	5-69
Learner Skills and Knowledge	5-69
Outline	5-70
Integrated IS-IS NET Addressing	5-71
Criteria and Path Selection for IS-IS Area Routing	5-73
Building an IP Forwarding Database	5-74
Example	5-75
Using show Commands	5-76
Summary	5-84
References	5-84
Quiz	5-85
Quiz Answer Key	5-87
Configuring Basic Integrated IS-IS	5-89
Overview	5-89
Relevance	5-89
Objectives	5-89
Learner Skills and Knowledge	5-89
Outline	5-90
Integrated IS-IS Configuration Steps	5-91
Basic IS-IS Configuration Commands	5-93
Example	5-96
Optimizing IS-IS	5-97
Example	5-100
Scalable IS-IS in Large Networks	5-101
Verifying IS-IS Configuration and Troubleshooting IS-IS Operations	5-102
Summary	5-104
References	5-104
Next Steps	5-104
Quiz	5-105
Quiz Answer Key	5-106
Lesson Assessments	5-107
Overview	5-107
Outline	5-107
Quiz 5-1: Overview of IS-IS Routing and CLNS	5-108
Objectives	5-108
Quiz	5-108
Scoring	5-108
Quiz 5-2: Understanding CLNS Addressing	5-109
Objectives	5-109
Quiz	5-109
Scoring	5-109
Quiz 5-3: Basic Operations of IS-IS in a CLNS Environment	5-110
Objectives	5-110
Quiz	5-110
Scoring	5-110
Quiz 5-4: Basic Operations of Integrated IS-IS in an IP and CLNS Environment	5-111
Objectives	5-111
Quiz	5-111
Scoring	5-111

Quiz 5-5: Configuring Basic Integrated IS-IS	5-112
Objectives	5-112
Quiz	5-112
Scoring	5-112
Lesson Assessment Answer Key	5-113

Table of Contents

Volume 3

<u>Manipulating Routing Updates</u>	6-1
Overview	6-1
Module Objectives	6-1
Module Outline	6-2
<u>Migration and Route Selection Between Multiple IP Routing Protocols</u>	6-3
Overview	6-3
Relevance	6-3
Objectives	6-3
Learner Skills and Knowledge	6-4
Outline	6-4
Considerations for Migrating to Another Routing Protocol	6-5
Example	6-6
Planning for New IP Address Allocation	6-7
Example	6-8
Procedures for Migrating to a New IP Address Space	6-9
Migrating to a New Routing Protocol	6-12
Purpose of Redistribution	6-14
Example	6-17
Seed Metrics	6-18
Redistribution Implementation Considerations	6-21
Summary	6-24
Quiz	6-25
Quiz Answer Key	6-27
<u>Configuring and Verifying Route Redistribution</u>	6-29
Overview	6-29
Relevance	6-29
Objectives	6-29
Learner Skills and Knowledge	6-30
Outline	6-30
Configuring Redistribution	6-31
The redistribute Command for RIP	6-33
Example	6-35
The redistribute Command for OSPF	6-36
Example	6-38
The redistribute Command for EIGRP	6-39
Example	6-41
The redistribute Command for IS-IS	6-42
Example	6-44
Example of Implementing and Verifying Route Redistribution	6-45
Summary	6-50
References	6-50
Quiz	6-51
Quiz Answer Key	6-53
<u>Controlling Routing Update Traffic</u>	6-55
Overview	6-55
Relevance	6-55
Objectives	6-55
Learner Skills and Knowledge	6-56
Outline	6-56
Passive Interface	6-57
Route Filtering	6-59
Example	6-61
Distribute List	6-62

Summary	6-66
Quiz	6-67
Quiz Answer Key	6-68
Using Route Maps to Control Routing Updates	6-69
Overview	6-69
Relevance	6-69
Objectives	6-69
Learner Skills and Knowledge	6-69
Outline	6-70
Route Map Operation	6-71
Example	6-75
route-map Commands	6-76
Route Maps with Redistribution	6-80
Example	6-81
Summary	6-82
Next Steps	6-82
Quiz	6-83
Quiz Answer Key	6-84
Using Administrative Distance to Influence the Route Selection Process	6-85
Overview	6-85
Relevance	6-85
Objectives	6-85
Learner Skills and Knowledge	6-85
Outline	6-86
Purpose of Administrative Distance	6-87
Example	6-88
Commands for Changing Administrative Distance	6-89
Examples of Redistribution Using Administrative Distance	6-91
Summary	6-97
Next Steps	6-97
Quiz	6-98
Quiz Answer Key	6-99
Policy-Based Routing	6-101
Overview	6-101
Relevance	6-101
Objectives	6-101
Learner Skills and Knowledge	6-101
Outline	6-102
Benefits of Policy-Based Routing	6-103
Establishing PBR Route Maps	6-105
Example of a PBR Configuration	6-114
Using PBR show and debug Commands	6-116
Summary	6-120
Next Steps	6-120
Quiz	6-121
Quiz Answer Key	6-122
Lesson Assessments	6-123
Overview	6-123
Outline	6-123
Quiz 6-1: Migration and Route Selection Between Multiple IP Routing Protocols	6-124
Objectives	6-124
Quiz	6-124
Scoring	6-125
Quiz 6-2: Configuring and Verifying Route Redistribution	6-126

Objectives	6-126
Quiz	6-126
Scoring	6-127
Quiz 6-3: Controlling Routing Update Traffic	6-128
Objectives	6-128
Quiz	6-128
Scoring	6-129
Quiz 6-4: Using Route Maps to Control Routing Updates	6-130
Objectives	6-130
Quiz	6-130
Scoring	6-132
Quiz 6-5: Using Administrative Distance to Influence the Route Selection Process	6-133
Objectives	6-133
Quiz	6-133
Scoring	6-133
Quiz 6-6: Policy-Based Routing	6-134
Objectives	6-134
Quiz	6-134
Scoring	6-135
Lesson Assessment Answer Key	6-136

Configuring Basic BGP 7-1

Overview	7-1
Module Objectives	7-1
Module Outline	7-2

BGP Overview 7-3

Overview	7-3
Relevance	7-3
Objectives	7-3
Learner Skills and Knowledge	7-3
Outline	7-4
Definition of BGP	7-5
BGP Path-Vector Routing	7-7
Example	7-9
BGP Characteristics	7-10
BGP Message Types	7-14
Summary	7-16
References	7-16
Quiz	7-17
Quiz Answer Key	7-18

BGP Concepts and Terminology 7-19

Overview	7-19
Relevance	7-19
Objectives	7-19
Learner Skills and Knowledge	7-19
Outline	7-20
Terminology for BGP Neighbor Relationships	7-21
External BGP Neighbors	7-22
Internal BGP Neighbors	7-23
Example	7-23
Full Mesh of IBGP Neighbors	7-24
Example	7-27
Summary	7-29
References	7-29
Quiz	7-30
Quiz Answer Key	7-31

Basic BGP Operations	7-33
Overview	7-33
Relevance	7-33
Objectives	7-33
Learner Skills and Knowledge	7-33
Outline	7-34
Basic BGP Configuration	7-35
Example	7-39
Example	7-43
Example	7-50
BGP Neighbor States	7-61
BGP show, debug, and clear Commands	7-66
Summary	7-75
Next Steps	7-75
Quiz	7-76
Quiz Answer Key	7-78
BGP Route Summarization	7-79
Overview	7-79
Relevance	7-79
Objectives	7-79
Learner Skills and Knowledge	7-79
Outline	7-80
BGP Version 4 and Classless Interdomain Routing	7-81
Example	7-84
BGP Route Summarization Using the network Command	7-85
Example	7-88
BGP Route Summarization Using the aggregate-address Command	7-89
Example	7-91
Summary	7-94
References	7-94
Quiz	7-95
Quiz Answer Key	7-97
BGP Path Selection Process	7-99
Overview	7-99
Relevance	7-99
Objectives	7-99
Learner Skills and Knowledge	7-99
Outline	7-100
Characteristics of BGP Attributes	7-101
The AS Path Attribute	7-105
Example	7-105
The Next-Hop Attribute	7-106
Example	7-106
The Origin Attribute	7-107
The Local Preference Attribute	7-108
Example	7-108
The MED Attribute	7-109
Example	7-109
The Weight Attribute	7-110
Example	7-110
BGP Path Selection Criteria	7-111
The BGP Path Selection Decision Tree	7-112
Summary	7-114
References	7-115
Next Steps	7-115

Quiz	7-116
Quiz Answer Key	7-118
Basic BGP Path Manipulation Using Route Maps	7-119
Overview	7-119
Relevance	7-119
Objectives	7-119
Learner Skills and Knowledge	7-119
Outline	7-120
Setting Local Preference with Route Maps	7-121
Setting the MED with Route Maps	7-132
Summary	7-139
Quiz	7-140
Quiz Answer Key	7-141
Design Options for Multihoming	7-143
Overview	7-143
Relevance	7-143
Objectives	7-143
Learner Skills and Knowledge	7-144
Outline	7-144
Design Choices with Multihoming for BGP	7-145
Default Route from Each Provider	7-147
Example	7-149
Partial Routing Table from Each Provider	7-150
Full Routing Table from Each Provider	7-153
Example	7-154
Summary	7-157
Next Steps	7-157
Quiz	7-158
Quiz Answer Key	7-159
Lesson Assessments	7-161
Overview	7-161
Outline	7-161
Quiz 7-1: BGP Overview	7-162
Objectives	7-162
Quiz	7-162
Scoring	7-162
Quiz 7-2: BGP Concepts and Terminology	7-163
Objectives	7-163
Quiz	7-163
Scoring	7-163
Quiz 7-3: Basic BGP Operations	7-164
Objectives	7-164
Quiz	7-164
Scoring	7-165
Quiz 7-4: BGP Route Summarization	7-166
Objectives	7-166
Quiz	7-166
Scoring	7-167
Quiz 7-5: BGP Path Selection Process	7-168
Objectives	7-168
Quiz	7-168
Scoring	7-169
Quiz 7-6: Basic BGP Path Manipulation Using Route Maps	7-170
Objectives	7-170
Quiz	7-170
Scoring	7-170

Quiz 7-7: Design Options for Multihoming	7-171
Objectives	7-171
Quiz	7-171
Scoring	7-171
Lesson Assessment Answer Key	7-172

Course Introduction

Overview

Building Scalable Cisco Internetworks (BSCI) v2.1 is recommended training for individuals seeking Cisco CCNP® certification. The course instructs network administrators of medium-to-large network sites on the use of advanced IP addressing and routing in implementing scalability for Cisco routers that are connected to LANs and WANs. The goal is to train network administrators to dramatically increase the number of routers and sites using these techniques instead of redesigning the network when additional sites or wiring configurations are added.

Outline

The Course Introduction includes these topics:

- Course Objectives
- Cisco Certifications
- Learner Skills and Knowledge
- Learner Responsibilities
- General Administration
- Course Flow Diagram
- Icons and Symbols
- Learner Introductions

Course Objectives

This topic lists the course objectives.

Course Objectives

Cisco.com

Upon completing this course, you will be able to:

- **Describe advanced IP addressing to include variable-length subnet masking, route summarization, classless interdomain routing, basic IP version 6, and use of Network Address Translation with route maps**
- **Identify advanced IP routing principles, including static and dynamic routing characteristics and the concepts of classless routing and network boundary summarization**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3

Upon completing this course, you will be able to:

- Describe advanced IP addressing to include variable-length subnet masking, route summarization, classless interdomain routing, basic IP version 6, and use of Network Address Translation with route maps
- Identify advanced IP routing principles, including static and dynamic routing characteristics and the concepts of classless routing and network boundary summarization

Course Objectives (Cont.)

Cisco.com

Upon completing this course, you will be able to:

- **Configure Enhanced Interior Gateway Routing Protocol for a scalable network**
- **Configure Open Shortest Path First for a scalable multiarea network**
- **Configure Intermediate System-to-Intermediate System for a scalable multiarea network**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4

Upon completing this course, you will be able to:

- Configure Enhanced Interior Gateway Routing Protocol for a scalable network
- Configure Open Shortest Path First for a scalable multiarea network
- Configure Intermediate System-to-Intermediate System for a scalable multiarea network

Course Objectives (Cont.)

Cisco.com

Upon completing this course, you will be able to:

- **Manipulate routing updates and packet flow using redistribution, distribution lists, administrative distance, route maps, and policy-based routing**
- **Configure basic Border Gateway Protocol for internal and external Border Gateway Protocol connections**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5

Upon completing this course, you will be able to:

- Manipulate routing updates and packet flow using redistribution, distribution lists, administrative distance, route maps, and policy-based routing
- Configure basic Border Gateway Protocol for internal and external Border Gateway Protocol connections

Cisco Certifications

This topic lists the certification requirements of this course.

A screenshot of a computer monitor displaying the Cisco Certifications website. The title 'Cisco Certifications' is at the top left. A large image shows a computer keyboard and monitor. At the bottom of the screen, the URL 'www.cisco.com/go/certifications' is displayed. The Cisco logo is in the top right corner of the page.

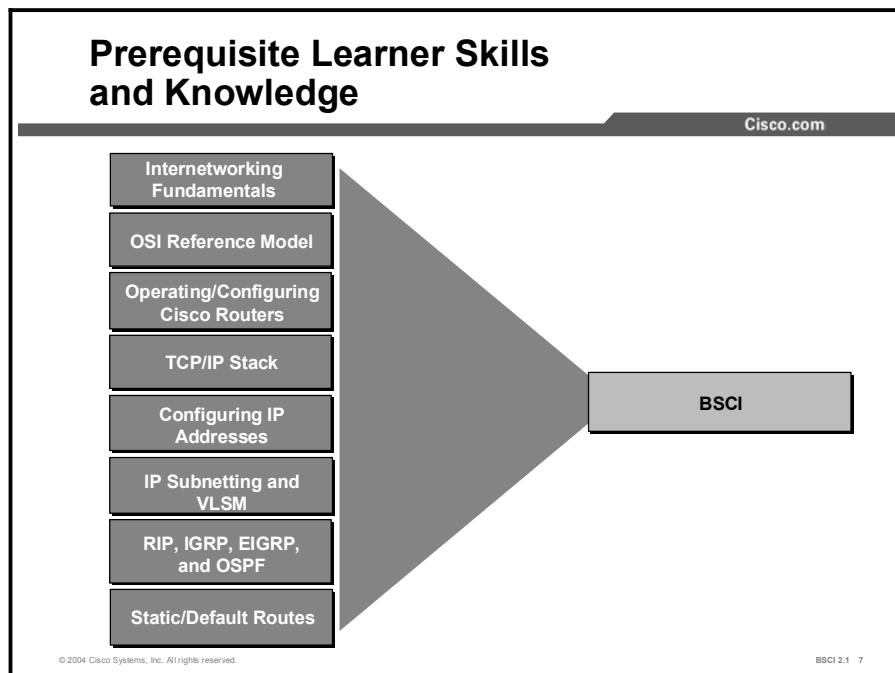
The screenshot shows a desktop computer setup with a monitor displaying the Cisco Certifications website. The website has a dark header with 'Cisco Certifications' and a 'Cisco.com' link. Below the header is a large image of a computer keyboard and monitor. At the bottom of the page, there is a dark banner with the text 'www.cisco.com/go/certifications'. The Cisco logo is visible in the top right corner of the website's content area.

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

- CCNA certification
- Networking terms, numbering schemes, and topologies
- Open Systems Interconnection (OSI) reference model
- Operating and configuring a Cisco router
- TCP/IP stack and configuration of IP addresses
- IP subnetting to include complex subnetting and variable-length subnet masking (VLSM)
- Routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks
- Using, implementing, and configuring static and default routes

Prerequisite Learner Skills and Knowledge (Cont.)

Cisco.com

- Interpreting a Cisco Routing Table
- Standard/Extended Access Lists
- Basic Router Configurations Using **show** and **debug** commands
- Configuring WANs with HDLC and PPP
- Configuring WANs Using Frame Relay PVCs

BSCI

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 8

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

- Interpreting the contents, entries, and indicators from a Cisco routing table
- Filtering traffic with standard and extended access lists
- Verifying basic router configurations using **show** and **debug** command output
- Verifying basic switch configurations using **show** command output
- Configuring a WAN serial interface using High-Level Data Link Control (HDLC) and PPP
- Configuring a WAN serial interface using Frame Relay permanent virtual circuits (PVCs) and subinterfaces

Learner Responsibilities

This topic discusses the responsibilities of the learners.

Learner Responsibilities

Cisco.com



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

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 9

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 <ul style="list-style-type: none">• Sign-in sheet• Length and times• Attire• Course materials	Facilities-Related <ul style="list-style-type: none">• Site emergency procedures• Rest rooms• Telephones/faxes• Break and lunchroom locations
---	---

© 2004 Cisco Systems, Inc. All rights reserved.

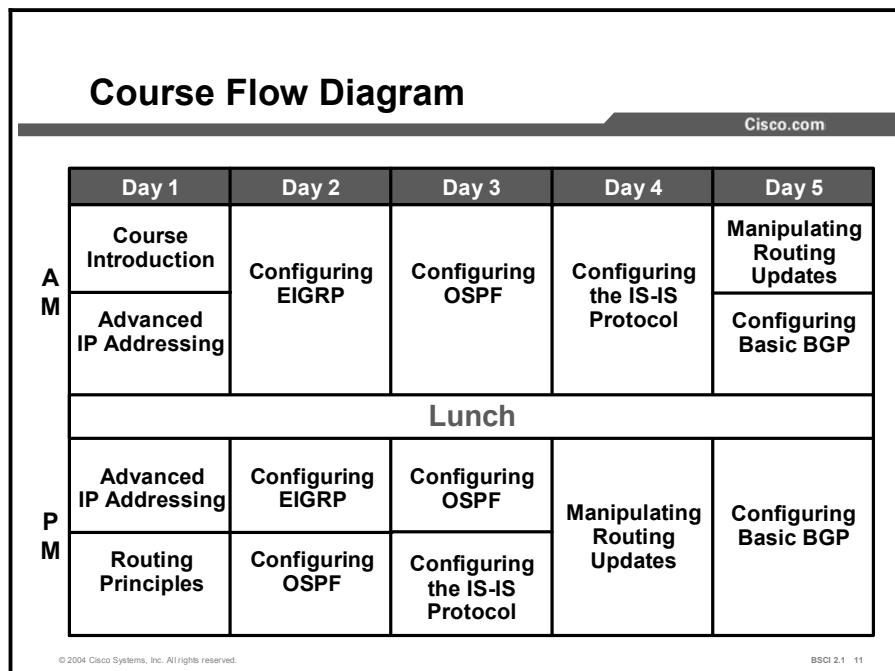
BSCI 2.1 10

The instructor will discuss the administrative issues noted here so 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 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 Diagram

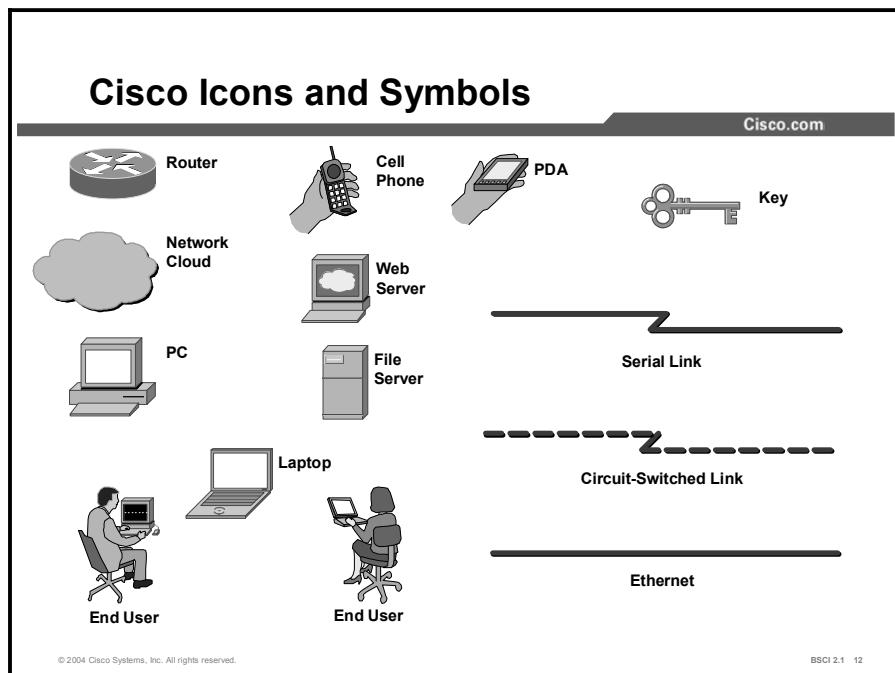
This topic covers the suggested flow of the course materials.



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 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



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 13

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

Module 1

Advanced IP Addressing

Overview

Scalable, well-behaved networks are not accidental; they are the result of good network design and effective implementation planning. A key element for effective scalable network implementation is a well-conceived and scalable advanced IP addressing plan. The purpose of an advanced IP addressing plan is to maximize the shrinking amount of IP address space available in deployed networks and minimize the size of routing tables.

As a network grows, the number of subnets and the volume of network addresses increase proportionally. Without advanced IP addressing technique, such as summarization and classless interdomain routing (CIDR), the size of the routing table is increased, which causes a variety of problems; for example, the network requires more CPU resources to acknowledge each internetwork topology change in a larger routing table. In addition, larger routing tables have greater potential for delays when the CPU resources sort and search for a match to a destination address. Both of these problems are solved by summarization and CIDR.

In order to effectively use summarization and CIDR to control the size of routing tables, network administrators employ advanced IP addressing techniques, such as Network Address Translation (NAT) and variable-length subnet masking (VLSM).

NAT uses globally unique addresses for routing across the Internet and between independent divisions within an organization. NAT uses different address pools for tracking groups of users, which makes it easier to manage interconnectivity.

VLSM is a type of subnet masking used for hierarchical addressing. This advanced IP addressing technique allows the network administrator to subnet a previously subnetted address to make the best use of the available address space.

Another long-standing problem that network administrators must overcome is the exhaustion of available IP addresses caused by the increase in Internet use. Although the current solution is to use NAT, the long-term solution is to migrate from the IP version 4 (IPv4) 32-bit address space to the IP version 6 (IPv6) 128-bit address space. Gaining an insight into IPv6 functionality and deployment will prove valuable for network administrators in the not-too-distant future.

Module Objectives

Upon completing this module, you will be able to maximize the shrinking amount of IP address space available in deployed networks and minimize the size of routing tables to provide a well-conceived and scalable advanced IP addressing plan.

Module Objectives

Cisco.com

- Explain the benefits and characteristics of an effective scalable IP-addressing plan
- Describe the role of variable-length subnet masking hierarchical addressing in a scalable network and calculate variable-length subnet masking
- Demonstrate the principles of route summarization and CIDR by summarizing a given range of network addresses into larger IP address blocks
- Describe the features and benefits of using IPv6, given the increasingly complex requirements of hierarchical addressing
- Configure NAT for multiple address pools using access lists and route maps

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-2

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- Purpose of Address Planning
- Hierarchical Addressing Using Variable-Length Subnet Masks
- Route Summarization and Classless Interdomain Routing
- Understanding IP Version 6
- Network Address Translation
- Lesson Assessments

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-3

Purpose of Address Planning

Overview

A well-designed large-scale internetwork with an effective scalable IP addressing plan has many benefits. These benefits include a network that is scalable, flexible, predictable, and able to hide information through summarization.

Relevance

You must execute a detailed IP addressing plan to increase the scale of a network in an optimal manner and take advantage of the advanced features of current IP routing protocols.

Objectives

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

- Explain the access, distribution, and core layer elements of network design in a scalable network
- List the advantages of effective network design principles
- Describe scalability, predictability, flexibility, and the ability to perform summarization as criteria of effective IP address planning

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

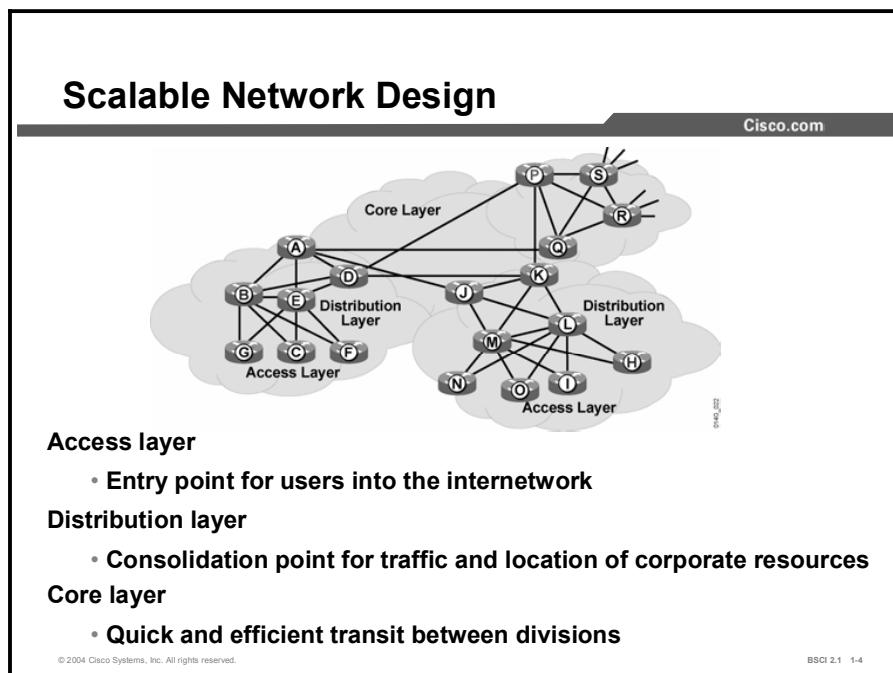
Cisco.com

- **Overview**
- **Scalable Network Design**
- **Benefits of Good Network Design**
- **Benefits of an Optimized IP Addressing Plan**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 1-3

Scalable Network Design

This topic covers the scalable network design concepts that are imperative for understanding IP address planning.



Corporate organizational structure affects the design of a network. The structure of scalable network design reflects the information flow of a corporation. These design structures are referred to as hierarchical network designs.

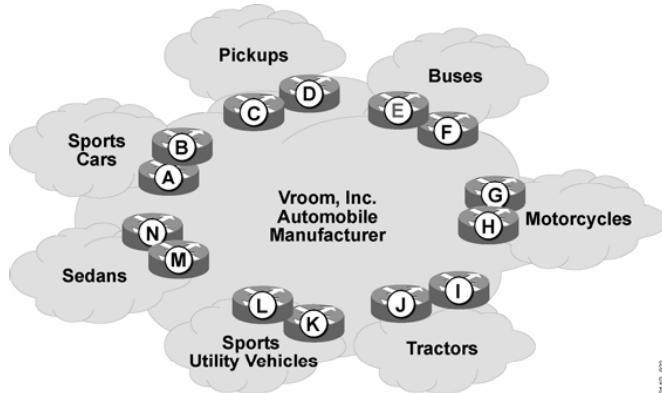
Two types of hierarchical network design are as follows:

- Functional
- Geographical

Within the context of these hierarchical networks, you must implement a scalable design at three network layers: the core layer, the access layer, and the distribution layer.

Functional Structured Design

Cisco.com



**Corporate networks may be organized by product divisions.
Network architecture can follow corporate organizational charts.**

©2004 Cisco Systems, Inc. All rights reserved.

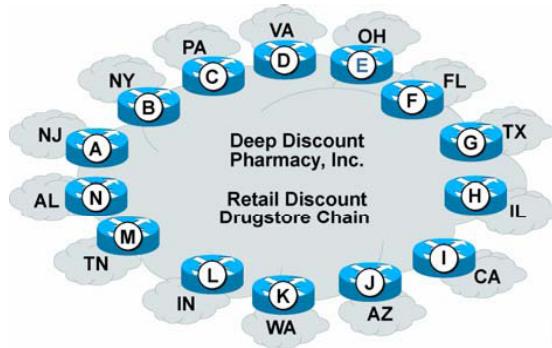
BSCI 2.1 1-8

Some corporations have independent divisions that are responsible for their own operations, including networking. These divisions interact with one another and share resources; however, each division has an independent chain of command.

This type of corporate structure is reflected in a functional network design. A functional design internetworks various divisions according to their functional purpose within the corporate structure.

Geographical Structured Design

Cisco.com



Networks are organized along geographical boundaries such as countries or states.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-6

Many interstate retail corporations are organized by geographical location of retail stores. Within the corporate structure, each local retail store reports to a district consolidation point. These district consolidation points report to regional consolidation points. The regional consolidation points then report to corporate headquarters.

This type of corporate structure is reflected in a geographical network design. A geographical design internetworks divisions according to their location.

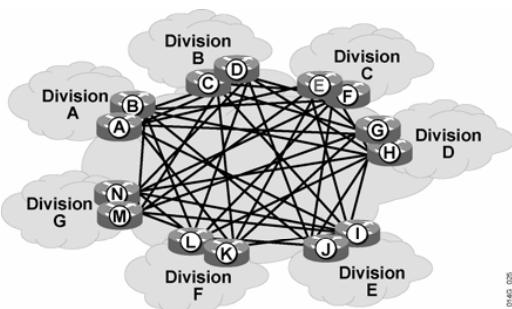
Note From a networking point of view, a geographical network structure is cost-effective because fewer network links require long-haul carriers, often a considerable added expense.

Within the functional or geographical networks, three primary layer elements are involved in a scalable network design:

- **Core layer:** The circuits with the largest bandwidth are in the core layer of the network. Redundancy occurs more frequently at this layer than at the other layers.
- **Access layer:** The access layer is the entry point into the network for end users and customers. VLANs, firewalls, and access lists maintain security for this layer.
- **Distribution layer:** The distribution layer is the consolidation point for access-layer devices. Host services with multiple access-layer devices are assigned to this layer.

Core Layer—Fully Meshed

Cisco.com



- The core layer is designed to provide quick and efficient access to headquarters and other divisions within the company.
- Redundancy is often found in the core network.
- Compared to other layers, the core generally has the circuits with the largest bandwidth.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-7

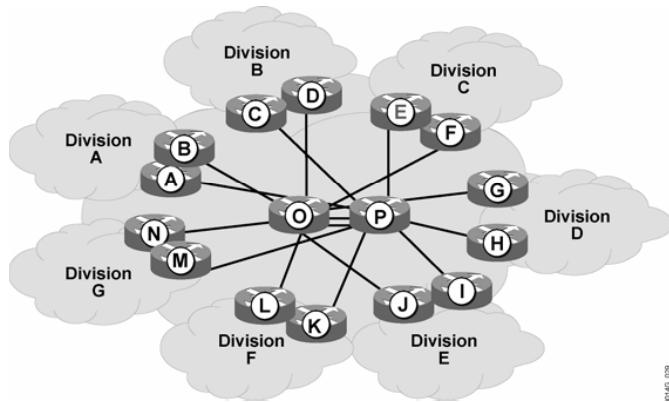
In the fully meshed core-layer design, each division has redundant routers at the core layer. The core sites are fully meshed together. For a small core with a limited number of divisions, this core-layer design provides robust connectivity. However, a fully meshed core-layer design is very expensive for a corporation with many divisions.

Note

In a fully meshed core-layer design, all routers have direct connections to all other nodes. This connectivity allows the network to react quickly when it must route data flow from a downed link to another pathway.

Core Layer—Hub-and-Spoke

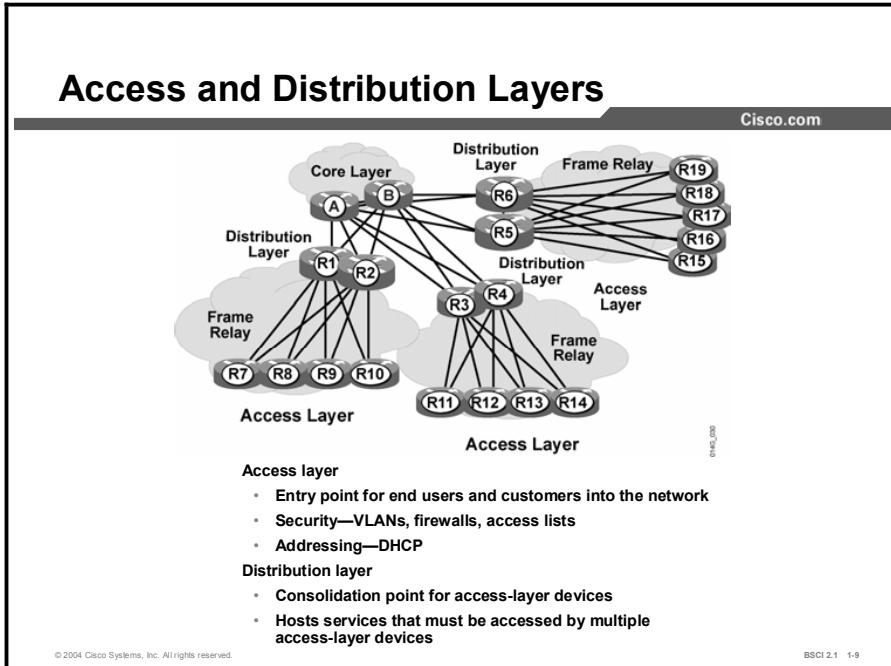
Cisco.com



四〇九

As the network grows, fully meshing all the core routers can become difficult. At that point, consolidation into geographically separate data centers is appropriate.

The hub-and-spoke design configuration supports the traffic flow through the corporation. In many companies, the data travels to a centralized headquarters, where the corporate databases and network services reside. To reflect this corporate centralization, the core-layer hub-and-spoke configuration establishes the focal point of the data flow as a key site.



Remote sites are points of entry to the network for end users and customers. Within the network, remote sites gain access to network services through the access layer. The distribution layer consolidates the services and devices that the access layer needs to process the activity that is generated by the remote sites.

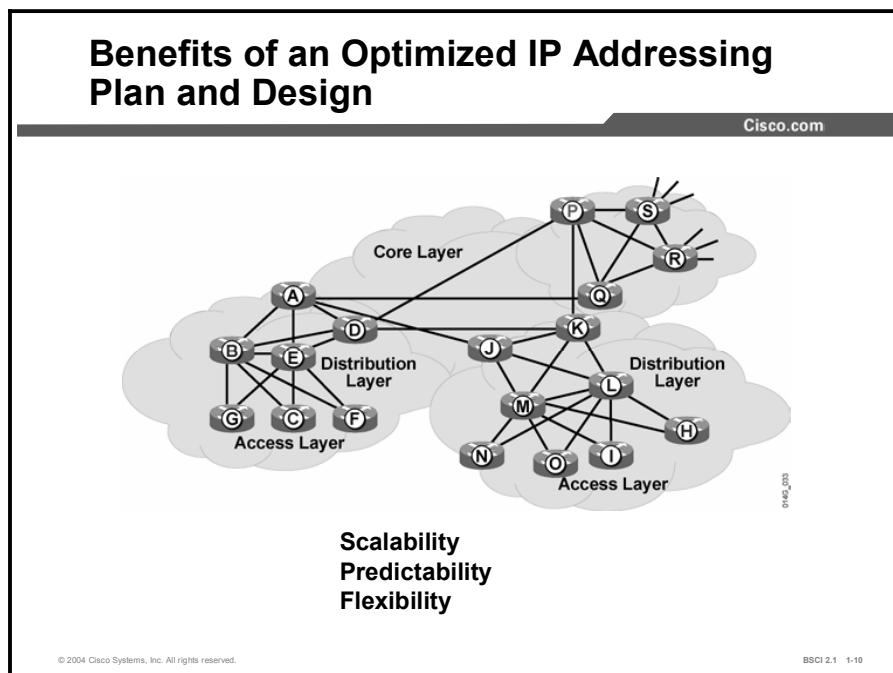
Place duplicating services at the distribution layer when there is no benefit in having duplicating services at the remote sites. These services may include Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), human resources, and accounting servers. One or more distribution layers report to each entry point at the core layer.

You can fully mesh connectivity between remote sites at the access layer. However, the hub-and-spoke configuration for remote sites reports to at least two corporate sites for administrative redundancy.

Note Frame Relay is the access protocol commonly used to interconnect geographically dispersed sites.

Benefits of Good Network Design

This topic describes the benefits of an effective IP addressing plan implemented within a good network design.



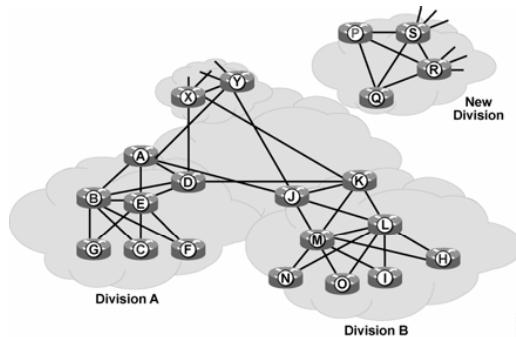
An effective network design accommodates unexpected growth and quick changes in the corporate environment. The network responds to mergers with other companies, corporate restructuring, and downsizing with minimal impact on the portions of the network that do not change.

The following are characteristics of good IP address plan implemented in a well-designed network:

- **Scalability:** A well-designed network allows for large increases in the number of supported sites.
- **Predictability:** A well-designed network exhibits predictable behavior and performance.
- **Flexibility:** A well-designed network minimizes the impact of routers, additions, changes, or removals within the network.

Scalability with Good Design

Cisco.com



- If one company merges with another company, where do you attach the additional routers?
 - If both companies were using network 10.0.0.0 for addressing, how would you overcome this obstacle and where would you implement the solution?

The current proliferation of corporate mergers emphasizes the design issues inherent in private IP addressing (RFC 1918). A scalable network that integrates private addressing with a good IP addressing plan minimizes the impact of additions or reorganizations of divisions within a network.

A scalable network enables companies that merge to connect at the core layer. Implementation of NAT on routers allows you to overlap network numbers and translate them to unused address space as a temporary solution. Then, overlapping network numbers can be changed on the PC or DHCP server.

RFC 1918 has set aside the following IP address space for private use:

- Class A network: 10.0.0.0 to 10.255.255.255
 - Class B network: 172.16.0.0 to 172.31.255.255
 - Class C network: 192.168.0.0 to 192.168.255.255

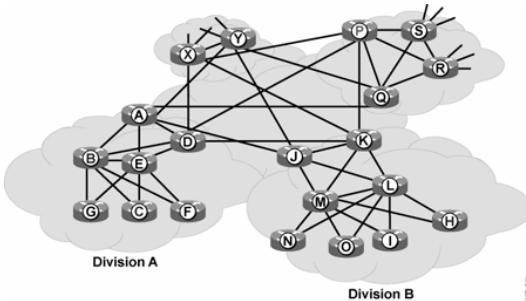
Note Private addressing is used exclusively for the examples in this course.

Good network design facilitates the process of adding routers to an existing network. In the example configuration, you can perform the following changes:

- Attach routers P and Q to the other routers in the core layer of the network
 - Change the IP address space of the new company from network 10.0.0.0 to network 172.16.0.0 and configure NAT on routers P and Q
 - Change the DHCP servers to reflect the newly assigned address space
 - Remove NAT from routers P and Q

Predictability with Good Design

Cisco.com



- The users behind routers B, C, and H are downloading 200 kbps per router from a server behind X. How much bandwidth do you need, and where do you place it to support this network?
- If router D fails, which pathways handle the new load?

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-12

The behavior of a scalable network is predictable. To gain predictability, bandwidth in a scalable network is equal to the higher-level site at each layer. For example, router C in the figure has the same bandwidth as routers B and E, so that router C fulfills load balancing. This load balancing allows access to networks behind routers B and E. Routers B and E are consolidation points for the access-layer routers (G, C, and F in the example).

The pathways between routers B and E and routers A and D need larger-bandwidth pipes to consolidate the traffic between corporate divisions. Because routers A and D consolidate multiple distribution points for this division, the connections for these routers to other divisions in the company need the largest bandwidth.

Use equal-cost paths for both hop count and bandwidth between any two routers in the internetwork; the packets load-balance across the internetwork. When a circuit or router fails, an alternate equal-cost path to the destination exists in every routing table. This alternate path limits convergence times and route recalculation to less than 1 second once a router discovers the failed circuit or router.

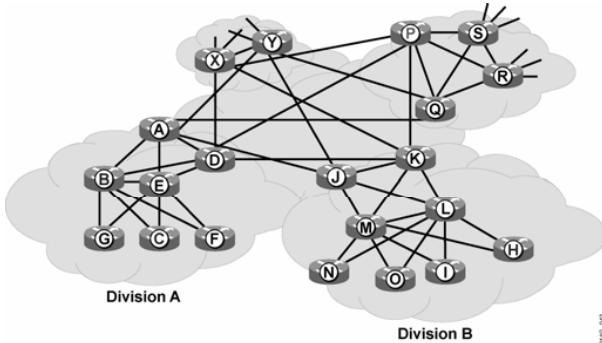
Routing Information Protocol (RIP) is an effective tool for implementing predictability in a well-designed scalable network. For example, consider a network where router C uses equal-cost hops to arrive at router X. The routing table for C has two best pathways to X: three hops through B and three hops through E.

If router D fails, the routing table for router C does not change. Router B and router E each have two best pathways to the networks behind router X: both have two hops through either router A or router D. These routers do not discover alternate routes because the preferred route exists in the routing table.

The result is a predictable traffic pattern. This level of network behavior predictability is a direct benefit of a scalable network design.

Flexibility with Good Design

Cisco.com



- Division B is sold and merged with another company, except for remote site H, which becomes part of Division A. How do you manage the transition?
 - What is the impact on the other divisions in the company?

Corporate reorganizations have little impact on the rest of the network when implemented in a scalable network. For example, assume an example network that uses Frame Relay at the remote sites.

The network administrator in the example network would accommodate a corporate reorganization with the following process:

- Install two additional virtual circuits from router H to routers B and E.
 - Following a successful installation, remove the virtual circuits to routers M and L.
 - Perform NAT on the router H interfaces to routers E and B to use the address space of Division A.
 - Remove the circuits from routers J and K to the other core routers A, D, P, Q, X, and Y.
 - Change the user addresses for router H to the new block of addresses.

Benefits of an Optimized IP Addressing Plan

This topic describes the benefits of a scalable network that can be realized when you implement an optimized IP addressing plan.

Benefits of Hierarchical Addressing

Cisco.com

- **Reduced number of route table entries:**
 - Summarize multiple addresses into route summaries
- **Efficient allocation of addresses:**
 - Contiguous address assignment allows you to use all possible addresses

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-14

The benefits of hierarchical addressing include the following:

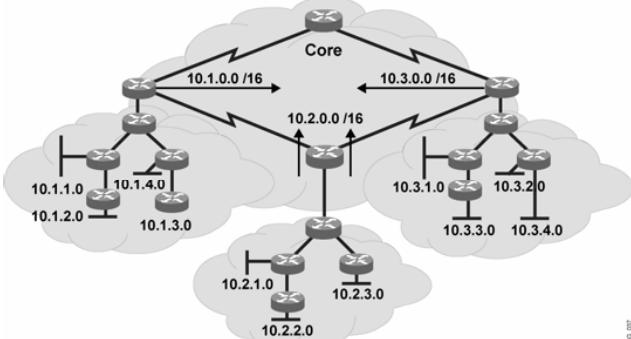
- **Reduced number of routing table entries:** With Internet routers and internal routers, routing tables are as small as possible because of route summarization. In a hierarchical addressing plan, route summarization allows an IP address to represent a collection of IP addresses. Route summarization makes routing table entries manageable and provides the following benefits:
 - More efficient routing
 - Reduced number of CPU cycles when recalculating a routing table or sorting through the routing table entries to find a match
 - Reduced router memory requirements
 - Faster convergence after a change in the network
 - Easier troubleshooting
- **Efficient allocation of addresses:** Hierarchical addressing allows you to take advantage of all available addresses by grouping the addresses contiguously. With random address assignment, addressing conflicts waste address groups. For example, classful routing protocols automatically create summary routes at a network boundary. These protocols do not support discontiguous addressing, which makes some addresses unusable if they are not assigned contiguously.

Within the context of hierarchical addressing, the IP network addressing plan must include provisions for summarization at key points. Summarization, or information hiding, is not a new concept. When a router announces a route to a given network, the route is a summarization of the addresses in the routing table for all the host devices and individual addresses that reside on that network.

Summarization helps reduce routing table size. The use of summarization to reduce the size of the routing table helps localize topology changes, a benefit that promotes network stability. Network stability occurs because a reduced routing table size means reduced bandwidth use. It also reduces memory use and the number of CPU cycles that are required to calculate the best path selection.

Scalable Network Addressing

Cisco.com



- Each of the 50 divisions has 200 /24 subnets.
- Each division summarizes its networks to 10.x.0.0 /16 on its core routers.
- The routing table for any router has 200 /24 subnets plus 49 /16 summarized routers for a total of 249 entries in the IP routing table.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-15

Example

For this example, assume the following:

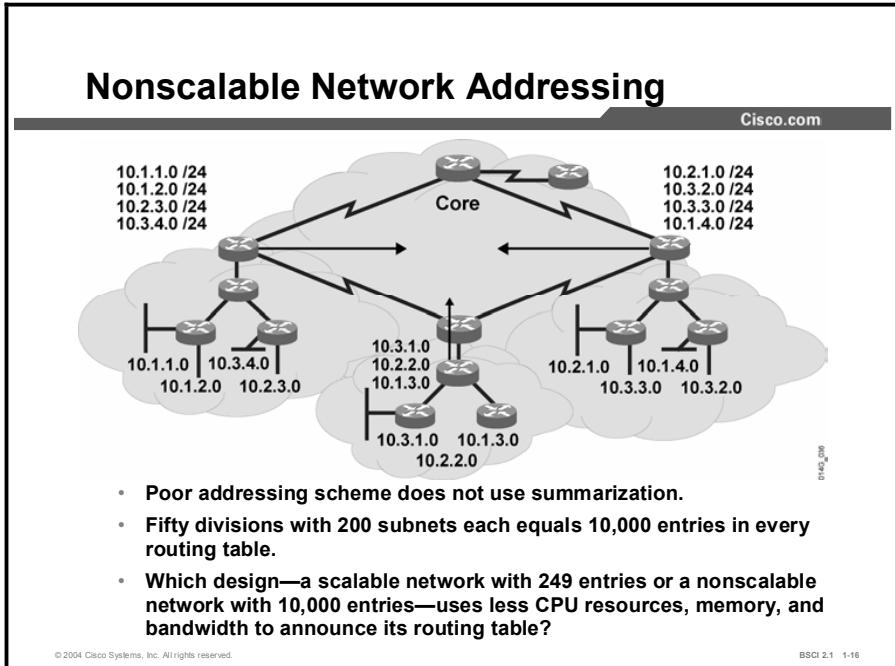
- A national drug store chain plans to have a retail outlet in every city in the United States with a population greater than 10,000.
- Each state has up to 100 stores, with two Ethernets in each store as follows:
 - One Ethernet tracks customer prescriptions, pharmacy inventory, and reordering stock.
 - The second Ethernet stocks the rest of the store and ties the cash registers into a corporate-wide, instantaneous point-of-sale evaluation tool.

The total number of Ethernet networks is 10,000 because there are 100 stores in 50 states, each with two Ethernets ($50 * 100 * 2 = 10,000$). This total does not include an equal number of serial links that interconnect these stores.

Using network address 10.0.0.0 and assigning a /24 subnet for each Ethernet creates an IP routing table of more than 10,000 subnets on each of the 5000 routers.

On the other hand, by using a scalable design and creating 51 divisions (one for each state and one for the backbone interconnecting the division), the drugstore chain can assign each division a block of 10.x.0.0 /16. Each Ethernet has a /24 subnet of network 10.0.0.0, and each division has 200 subnets in the IP routing table of each router.

When each division summarizes the block of network 10.x.0.0 /16 at the entry point to the core network, any router in a division can see the 200 /24 networks that represent the subnets for that division and 49 10.x.0.0 /16 summarizations that represent each additional division. This provides a total of 249 networks in each IP routing table.



When you do not use summarization to assign IP addresses, problems occur. As shown in this figure, a network with 50 divisions in a scalable network with summarization has 249 routes in every routing table. The same network without summarization has 10,000 routes in every routing table. Why is the large number of routes a problem? The problems relate to the frequency and size of routing table updates and the way that topology changes are processed in summarized and unsummarized networks.

Update Size

Routing protocols such as RIP and Interior Gateway Routing Protocol (IGRP), which send a periodic update every 30 and 90 seconds, respectively, use valuable bandwidth to maintain a table without summarization. RIP can fit 25 networks in each update; therefore, 10,000 networks can have RIP on every router creating and sending 400 packets every 30 seconds. When these routes summarize, the table of 249 networks sends only 10 packets every 30 seconds, compared to the 400 packets from the unsummarized routing table.

Unsummarized Internetwork Topology Changes

A routing table with 10,000 entries constantly changes. To illustrate this constant change, consider a network that has more than 5000 routers, with at least one at 5000 different sites. Something changes somewhere in the network every day, for example, a power outage occurs at site A; a backhoe digs a trench at site B; a newly hired system administrator begins work at site C; a Cisco IOS software upgrade is in progress at site D; and a newly added router is being installed at site E.

There are other examples of this negative impact as well. For example, when you are using a routing protocol such as Open Shortest Path First (OSPF), an upgrade or topology change on the internetwork causes a shortest path first (SPF) calculation. The SPF calculations are large, because each router needs to calculate all known pathways to each of the 10,000 networks. Each change that a router receives requires time and CPU resources.

Summarized Network Topology Changes

In contrast to an unsummarized network, a summarized network responds efficiently to network changes. For example, in a network with 200 routers for a corporate division, the routers see all the subnets for that division. When a change occurs to one of the 200 routers in the division, all other routers in the division recalculate to reflect the topology change of those affected networks.

The core routers of that division pass a summarized /16 route and suppress only the /24 networks from advertisement to the core routers of other divisions. The summarized route is announced as long as a portion of the summarized block is reachable from that core router. The more specific routes are suppressed, so that changes from this division are not propagated to other divisions.

In this scenario, each router recognizes only 200 /24 networks and not the 10,000 /24 networks in an unsummarized environment. Obviously, the CPU resources, memory, and bandwidth required for the 200 networks is less than for the 10,000 networks. With summarization, each division hides more specific information from the other divisions and passes only the summarized route that represents that overall division.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Networks must be designed to support the benefits found in advanced IP routing protocols.
- Well-designed networks allow corporations to react quickly to changes in their networking requirements. These changes can be mergers, reorganizations, or downsizing.
- A hierarchical design approach and good IP address planning give scalable networks the capability to grow and to be broken up into autonomous operating units.

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 which layer are you most likely to see large bandwidth, redundant equipment, and redundant circuits?
- A) access layer
 - B) core layer
 - C) distribution layer
- Q2) At which layer is consolidation performed?
- A) access layer
 - B) core layer
 - C) distribution layer
- Q3) At which layer would you find PCs and print servers?
- A) access layer
 - B) core layer
 - C) distribution layer
- Q4) Which three of the following statements are benefits of good network design? (Choose three.)
- A) the ability to manage the network as it grows to a large size
 - B) the ability to predict the behavior of network
 - C) the ability to adapt to topology changes quickly and efficiently
 - D) detailed knowledge of all networks and subnetworks
- Q5) Which four benefits are reasons to reduce the size of the routing table by using route summarization? (Choose four.)
- A) more efficient routing
 - B) reduced number of CPU cycles when recalculating or sorting through the routing table entries to find a match
 - C) reduced router memory requirements
 - D) job security
 - E) faster convergence after a change in the network
 - F) easier troubleshooting

Quiz Answer Key

Q1) B

Relates to: Scalable Network Design

Q2) C

Relates to: Scalable Network Design

Q3) A

Relates to: Scalable Network Design

Q4) A, B, C

Relates to: Benefits of Good Network Design

Q5) A, B, C, E

Relates to: Benefits of an Optimized IP Addressing Plan

Hierarchical Addressing Using Variable-Length Subnet Masks

Overview

Variable-length subnet masking (VLSM) is a crucial component of an effective IP-addressing plan for a scalable network. This lesson introduces VLSM, provides examples, and discusses methods of determining the best subnet mask for a given address requirement.

Relevance

Calculating a large-enough subnet and determining the range of addresses for a given set of devices are imperative for implementing a scalable network. Understanding VLSM and how to implement it are fundamental to understanding route summarization and CIDR. Once implemented, VLSM is essential for configuring and troubleshooting advanced IP routing protocols and related routing tables.

Objectives

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

- Define the purpose of VLSM
- Explain how to use VLSM to maximize the use of the limited number of IP addresses
- Explain the steps involved in VLSM calculation

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- An understanding of IP subnetting, including complex subnetting

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Prefix Length and Network Mask**
- **Implementing VLSM in a Scalable Network**
- **Calculating VLSM**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-3

Prefix Length and Network Mask

The concept of a network mask and the prefix length field specifically relate to hierarchically addressed network implementation. This topic discusses the purpose of the network mask and the prefix length field and describes their use within a network.

Prefix Length and Network Mask

Cisco.com

Range of addresses: 192.168.1.64 through 192.168.1.79

- Have the first 28 bits in common, which is represented by a /28 prefix length
- 28 bits in common can also be represented in dotted decimal as 255.255.255.240

Binary ones in the network mask represent network bits in the accompanying IP address; binary zeros represent host bits

11000000.10101000.00000001.0100xxxx	IP address
11111111.11111111.11111111.11110000	Network mask

In the IP network number that accompanies the network mask, when the host bits of the IP network number are:

- All binary zeros—That address is the bottom of the address range
- All binary ones—That address is the top of the address range

Fourth Octet

64	01000000
65	01000001
66	01000010
67	01000011
68	01000100
69	01000101
70	01000110
71	01000111
72	01001000
73	01001001
74	01001010
75	01001011
76	01001100
77	01001101
78	01001110
79	01001111

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 1-4

The network mask and the prefix length field inform a device of the range of addresses associated with a corresponding IP address.

A series of contiguous ones from left to right in a routing mask defines how many bits in the corresponding IP address belong to the network number. The series of contiguous zeros that follows represents the host bits in the corresponding IP number. When you add bits to the network part of an address to make the all-ones field longer, the number of bits in the host part of the address decreases. You create additional networks (subnets) at the expense of the number of host devices that can occupy each network segment.

The number of bits that you add to the default routing mask creates a counting range for subnets. Each count is a unique binary pattern. The number of subnetworks created is calculated by the 2^n formula, where n is the number of bits by which the default routing mask is extended. You must use the configuration commands in Cisco IOS software releases earlier than Software Release 12.0 to explicitly allow subnetwork 0. In Cisco IOS Software Release 12.0 and later, subnetwork 0 is enabled by default.

The bits that are not allocated as the network part or the subnetwork part of the address form a counting range for hosts. Host addresses are selected from these remaining bits and must also be numerically unique from all other hosts on the network.

Note	The number of hosts created is calculated by the formula $2^n - 2$, where n is the number of bits available in the host portion. In the host counting range, the all-zeros pattern is reserved as the subnet identifier, and the all-ones pattern is reserved as a broadcast address to reach all hosts.
-------------	---

Both the IP address and the associated routing mask contain 32 bits. Routing devices are similar to computers in that they both use the binary numbering scheme to represent addresses. Working with 32-bit binary numbers is the standard operational mode for a routing device. However, network administrators do not use binary numbers on a daily basis and have adopted other formats to represent 32-bit IP addresses. Some common formats include decimal (base 10) and hexadecimal (base 16) notation.

The generally accepted method of representing IP address and routing masks is to break the 32-bit field into four groups of 8 bits and to represent those 8-bit fields in a decimal format separated by decimal points. This method of representing IP address and routing mask is called 32-bit dotted-decimal notation.

Although dotted decimal notation is commonly accepted practice , the routing device internally uses the 32-bit binary string as an address identifier. All routing decisions are based on the 32-bit binary field.

Example

If a PC has an IP address of 192.168.1.67 with a mask of 255.255.255.240 or a prefix length of /28, it uses this value to determine which other devices with host addresses on the local connection have the first 28 bits in their IP address in common. The PC uses Address Resolution Protocol (ARP) to find the corresponding MAC address if communication with any of these devices is necessary. The range of these local devices is 192.168.1.64 through 192.168.1.79. If a PC sends information to an IP device that is not in the range, the IP forwards the information to its default gateway.

A router behaves in a similar manner when it makes a routing decision. A packet arrives on the router and is passed to the routing table. The router compares the destination IP of the packet address to network entries in the routing table. These network entries have a prefix length associated with them. The router uses the prefix length to determine how many destination address bits must match to take the corresponding outbound interface that is associated with that network number in the routing table.

Consider the following scenario in which an IP packet with a destination address of 192.168.1.67 is sent to the IP routing table of a router:

- 192.168.1.0 is subnetted, four subnets
- O 192.168.1.16/28 [110/1800] via 172.16.1.1, 00:05:17, serial 0
- C 192.168.1.32/28 is directly connected, Ethernet 0
- O 192.168.1.64/28 [110/10] via 192.168.1.33, 00:05:17, Ethernet 0
- O 192.168.1.80/28 [110/1800] via 172.16.2.1, 00:05:17, serial 1

In this example, the router determines where to send a packet that is destined for 192.168.1.67. The routing table has four entries for network 192.168.1.0. The router compares the destination address to each of the four entries for this network. The destination address matches the first 24 bits of each of these entries.

Notice that, in the list that follows, the number 67 matches the first 25 bits of each network number. The number 67 does not match the first 26 bits for networks 16 and 32, but it does match the first 26 bits for 64 and 80. Address 192.168.1.67 matches all 28 bits of network address 192.168.1.64. To use this network, the destination address needs to match the first 28 bits in the network number, so the router forwards this packet to the next router (192.168.1.33) on the Ethernet 0 interface.

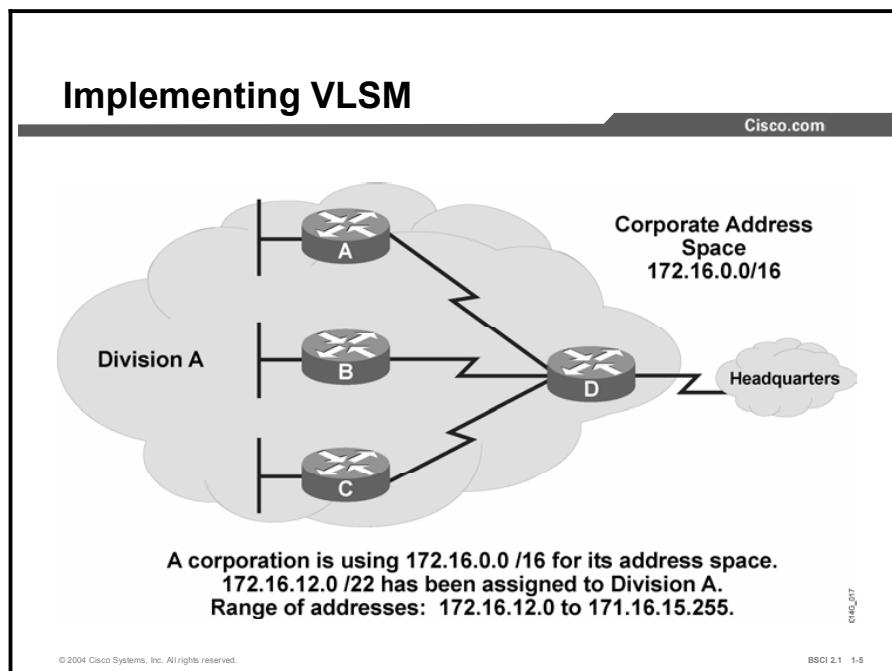
The destination address of 192.168.1.67 has the first three octets in common with all four entries in the routing table, but it is not clear by looking at the decimal representation which of those entries is the best match to route this packet. A router handles all packets in binary, not dotted decimal notation.

Following is the binary representation of the last octet for destination address 192.168.1.67 and the binary representation of the last octet for the four entries in the IP routing table. Since the prefix length is 28 and all four entries match to at least the first 24 bits of 192.168.1, the object is to find the routing table entry that matches the first four bits of the number 67. It is not important whether the last four bits match, so the target is 0100xxxx. (Note that the routing entry of 64, which has a value of 0100 in the first four bits, is the only one that matches this requirement.)

- 67: 01000011
- 16: 00010000
- 32: 00100000
- 64: 01000000
- 80: 01010000

Implementing VLSM in a Scalable Network

This topic discusses the importance of VLSM in a scalable network and explains the process to calculate the appropriate network mask for a given number of host devices.



VLSM allows more than one subnet mask within a network and enables the subnetting of a previously subnetted network address. Characteristics that permit VLSM to conserve IP addresses include the following:

- **Reduced number of routing table entries:** For both Internet routers and internal routers, use route summarization to keep routing tables as small as possible. In a hierarchical addressing plan, route summarization allows a single IP address to represent a collection of IP addresses. Route summarization keeps routing table entries manageable and provides the following benefits:
 - More efficient routing
 - Reduction in the number of CPU cycles needed to sort through the routing table entries to find a match and recalculate a routing table
 - Reduction in router memory requirements
 - Faster convergence after a change in the network
 - Easier troubleshooting
- **Greater capability to use route summarization:** VLSM allows more hierarchical levels within an addressing plan. More hierarchical levels result in better route summarization within the routing tables. For example, subnet 172.16.12.0/22 in the figure summarizes all the addresses that are further subnets of 172.16.12.0/22, including those from subnet 172.16.14.0/27 and 172.16.14.128/30.
- **Efficient use of IP addresses:** Hierarchical addressing provides the advantage of using all possible addresses because the addresses are grouped contiguously. With random address

assignment, addressing conflicts can waste groups of addresses. For example, recall that classful routing protocols automatically create summary routes at a network boundary. These protocols do not support discontiguous addressing, so some addresses are unusable if you do not assign them contiguously.

Companies that do not use VLSM must implement a single subnet mask within an entire Class A, B, or C network number, as follows:

- A network architect decides to use the 172.16.0.0/16 network address space to design a corporate network. The architect divides it into blocks of 4 /24 networks. The resulting 256 networks, divided by 4, create 64 blocks of addresses with up to 1024 hosts in each block.
- The network architect assigns Division A to address block 172.16.12.0/22. The prefix mask of /22 indicates that all addresses within that range have the first 22 bits in common when reading from left to right. The prefix mask provides Division A with a range of addresses from 172.16.12.0 through 172.16.15.255.

Example

Range Of Addresses for VLSM	
Cisco.com	
Subnetted Address: 172.16.12.0 /22	
Dotted Decimal Notation	Binary Notation
172.16.11.0	10101100. 00010000.00001011.00000000
(Text omitted for continuation of bit/number pattern)	
172.16.12.0	10101100. 00010000.00001100.00000000
172.16.12.1	10101100. 00010000.00001100.00000001
172.16.12.255	10101100. 00010000.00001100.11111111
172.16.13.0	10101100. 00010000.00001101.00000000
172.16.13.1	10101100. 00010000.00001101.00000001
172.16.13.255	10101100. 00010000.00001101.11111111
172.16.14.0	10101100. 00010000.00001110.00000000
172.16.14.1	10101100. 00010000.00001110.00000001
172.16.14.255	10101100. 00010000.00001110.11111111
172.16.15.0	10101100. 00010000.00001111.00000000
172.16.15.1	10101100. 00010000.00001111.00000001
172.16.15.255	10101100. 00010000.00001111.11111111
(Text omitted for continuation of bit/number pattern)	
172.16.16.0	10101100. 00010000.00010000.00000000

© 2004 Cisco Systems, Inc. All rights reserved.

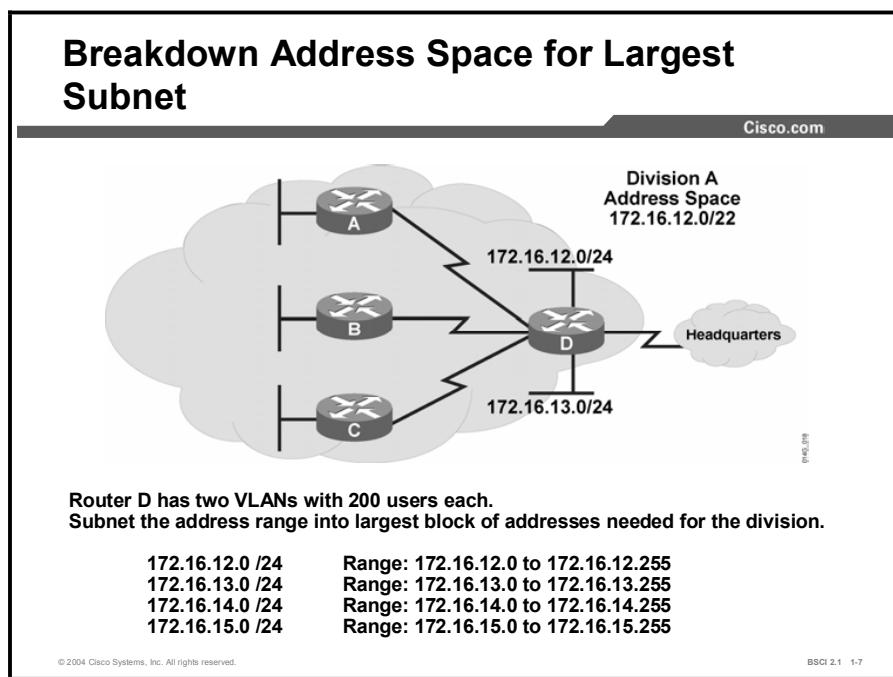
BSCI 2.1 1-6
0140_423

The figure displays the binary representation of networks 172.16.11.0 through 172.16.16.0. Notice that networks 172.16.12.0 through 172.16.15.255 all have the first 22 bits in common. Network 172.16.11.0 and network 172.16.16.0 do not have these first 22 bits in common.

Compare these two addresses to those used by Division A in the previous figure, and note that neither address is part of the address space that Division A can use. These networks are outside the range of addresses that are part of the VLSM block because they do not share the same 22 bits that are common to networks 172.16.12.0 through 172.16.15.255.

Calculating VLSM

You can best understand the design and implementation of a scalable IP address plan if you study a detailed example of how a VLSM network is laid out. This topic discusses the steps to design and implement a scalable IP address plan.



The steps for designing and implementing a scalable IP address plan are as follows:

- Step 1** Assign a summarized block of addresses to create a portion of a corporate network and subnet for the 200-user VLANs.
- Step 2** Resubnet the remaining address space for three 24-port Ethernet switches.
- Step 3** Subnet a portion of the remaining address space a third time to address three point-to-point serial links.

With VLSM, you can subnet the 172.16.12.0/22 address to provide more network addresses and fewer hosts per network. For example, if you subnet address 172.16.12.0/22 to 172.16.12.0/24, you gain 4 (2^2) subnets, each of which supports 254 (2^{8-2}) hosts.

To start the VLSM process, determine the largest subnet necessary for the networks to which you assign IP addresses. Determine the number of hosts necessary per subnetwork by completing the following steps:

- Step 1** Check corporate policy to see if a limit is set per segment or VLAN.
- Step 2** Check the physical number of ports on a switch.
- Step 3** Check the current size of the network or networks at other sites that fulfill the same role.

To determine the size of the block of addresses to assign to a network, complete the following steps:

- Step 1** Calculate the maximum number of hosts on that wire.
- Step 2** Add 2 to that number to account for the broadcast and network numbers.
- Step 3** Round up to the next higher power of 2.

Because IP addresses are binary, you must divide them into powers of 2. A block of addresses is 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, and so on. Perform subnetting with blocks of 4, 8, 16, 32, 64, 128, and 256. You lose two addresses each time you create a subnet: one for the network number and the other for the broadcast address.

The bottom address of the range, where the host bits are all zeros, is the network number. The top of the address range, where the host bits are all ones, is the broadcast address. The number of addresses in a block that are assignable to devices is: $4 - 2 = 2$; $8 - 2 = 6$; $16 - 2 = 14$; $32 - 2 = 30$; $64 - 2 = 62$; $128 - 2 = 126$; and $256 - 2 = 254$.

In the example, the network administrator subnets the 172.16.12.0 /22 into 4 /24 subnets on router D; one of the subnets is for VLAN 1 and another for VLAN 2. This subnetting leaves two /24 subnets to use for the 24-port switches at the three remote sites and the three serial point-to-point links. After you establish the VLANs, you must assign Ethernets for the remote site. The purchasing agent buys 24-port Cisco Catalyst 2924 10/100 Ethernet switches. Company policy does not allow hubs; rather, you assign each device its own port on an Ethernet switch. Corporate management guarantees that the number of users at each remote site does not exceed 20. The calculation for a maximum of 20 users is as follows:

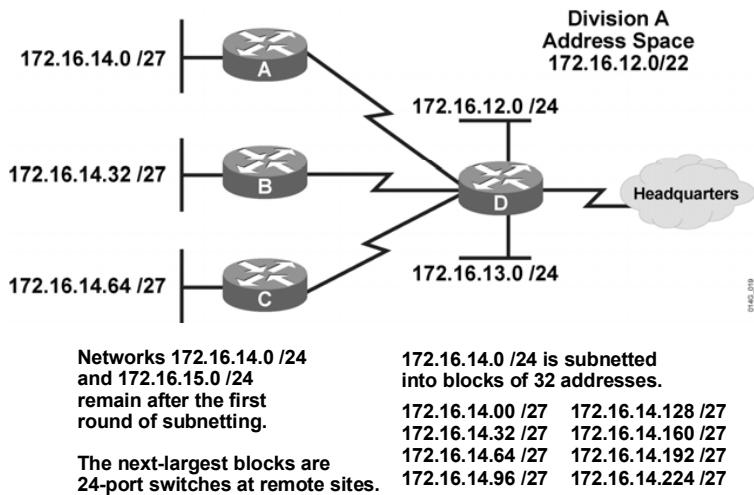
- Step 1** Add 2 to 20 and round up to the next higher power of 2, which is 32.
- Step 2** Calculate 5 host bits for 30 hosts per subnetwork, because 32 is 2 to the power of 5.
- Step 3** Subtract 5 host bits from a total of 32 bits (in an IP address) to give a network mask of /27.

You cannot use the 172.16.12.0/24 or 172.16.13.0/24 networks because they are assigned to VLANs 1 and 2 on router D. Networks 172.16.14.0/24 and 172.16.15.0/24 are available for resubnetting.

If you resubnet 172.16.14.0/24 into /27 subnets, you will achieve the subnets in the diagram.

Breakdown Address Space for Ethernets at Remote Sites

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-8

Administrators commonly use VLSM 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 conserves scarce IP addresses.

In the figure, subdividing the 172.16.14.0/24 subnet into multiple /27 subnets generates the subnet addresses on the Ethernets. The figure illustrates where the subnet addresses are applied, depending on the number of host requirements.

Once you establish the Ethernet switches at the remote sites, you must address the wire serial links between the remote sites and router D. The serial links are point-to-point Frame Relay and need an IP address for each side. Because the serial links require two addresses, add two more addresses for the network number and the broadcast address. Then, if necessary, round up to the next higher power of 2.

In this case, there is no need to round up because the sum of the numbers is 4, and 4 is 2 to the power of 2. Therefore, 2 host bits allow for two hosts per subnetwork number. Subtracting 2 host bits from the total of 32 bits in an IP address results in a network mask of /30 ($32 - 2 = 30$). In the example, the WAN links use subnet addresses with a prefix of /30. This prefix allows for two hosts only—just enough hosts for a point-to-point connection between a pair of routers.

To calculate the subnet addresses for the WAN links, further subnet one of the unused /27 subnets. In this example, 172.16.14.224/27 is further subnetted with a prefix of /30. If you subnet these subnets, it provides three more subnet bits. Therefore, eight (2^3) subnets for the WANs are available.

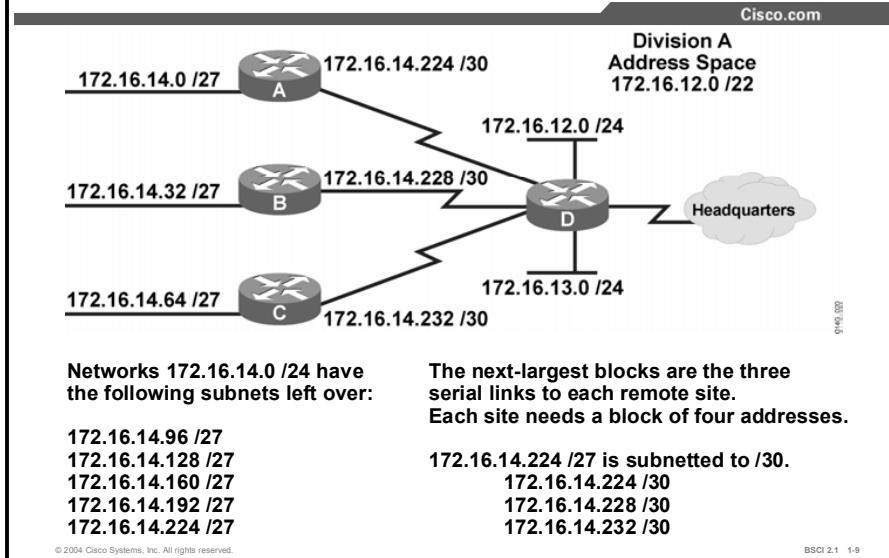
Note It is important to remember that only unused subnets can be further subnetted. In other words, if you use any addresses from a subnet, that subnet cannot be further subnetted. In the example, three subnet numbers are used on the LANs. Another unused subnet, 172.16.14.224/27, is further subnetted for use on the WANs.

The 172.16.15.0/24 block for these /30 subnets can be used, but only three subnets are currently needed. In this example, a good use of address space would be to address a division with 40 remote sites by dividing a /24 network into 64 /30 subnets. Since you need only three subnets, you can take one of the leftover /27 subnets of 172.16.14.x and resubnet it to /30, which provides eight subnets. The outcome is three serial links that have addresses, with five /30 subnets left over for possible expansion.

To provide the most flexibility for future growth, select the 172.16.14.224/27 subnet instead of the next available subnet of 172.16.14.96. If the company purchases more switches, the next switch is assigned the 172.16.14.96/27 subnet, and the new remote site is connected to router D with the 172.16.14.236/30 serial subnet.

Another solution is to add three more /27 subnets and three /30 serial links before the company needs to use the 172.16.15.0/24 subnet. The 172.16.15.0/24 subnet can be reserved for another VLAN or more remote sites.

Break Down Remaining Address Space for Serial Subnets



When you subnet the 172.16.14.224/27 subnet into multiple subnets with a /30 mask, it results in eight /30 subnets. Notice that all eight subnet addresses have the first 27 bits in common and are part of the 172.16.14.224 /27 subnet. If you use the first three /30 subnets, then five /30 subnets remain.

Assignments of subnets, serial links, and routers in the figure are as follows:

- 172.16.14.224/30 network for the serial link between router A and router D
- 172.16.14.228/30 subnet for the serial link between router B and router D
- 172.16.14.232/30 subnet for the serial link between router C and router D

Address information for router A to router D is as follows:

- **Network number:** 172.16.14.224
- **Router A serial interface:** 172.16.14.225
- **Router D serial interface:** 172.16.14.226
- **Broadcast address for network 172.16.14.224/30:** 172.16.14.227

Address information for router B to router D is as follows:

- **Network number:** 172.16.14.228
- **Router B serial interface:** 172.16.14.229
- **Router D serial interface:** 172.16.14.230
- **Broadcast address for network 172.16.14.228/30:** 172.16.14.231

Address information for router C to router D is as follows:

- **Network number:** 172.16.14.232
- **Router C serial interface:** 172.16.14.233
- **Router D serial interface:** 172.16.14.234
- **Broadcast address for network 172.16.14.232/30:** 172.16.14.235

Example

Calculating VLSM: Binary					
Cisco.com					
VLSM Addresses for /24 for 172.16.12.0 – 172.16.15.255 :					
172.16.12.0	10101100. 00010000.000011	00 .0000000	00 .0000000	VLAN 1	
172.16.13.0	10101100. 00010000.000011	01 .0000000	01 .0000000	VLAN 2	
172.16.14.0	10101100. 00010000.000011	10 .0000000	Nodes		
172.16.15.0	10101100. 00010000.000011	11 .0000000	Not used		
VLSM Addresses for /27 for 172.16.14.0 – 172.16.14.255:					
172.16.14.0	10101100. 00010000.000011	10 .000	00000	Nodes Site A	
172.16.14.32	10101100. 00010000.000011	10 .001	00000	Nodes Site B	
172.16.14.64	10101100. 00010000.000011	10 .010	00000	Nodes Site C	
VLSM Addresses for /30 for 172.16.14.224 – 172.16.14.255:					
172.16.14.224	10101100. 00010000.000011	10 .111	000 00	A-D Serial	
172.16.14.228	10101100. 00010000.000011	10 .111	001 00	B-D Serial	
172.16.14.232	10101100. 00010000.000011	10 .111	010 00	C-D Serial	
172.16.14.236	10101100. 00010000.000011	10 .111	011 00	Not used	
172.16.14.240	10101100. 00010000.000011	10 .111	100 00	Not used	
172.16.14.244	10101100. 00010000.000011	10 .111	101 00	Not used	
172.16.14.248	10101100. 00010000.000011	10 .111	110 00	Not used	
172.16.14.252	10101100. 00010000.000011	10 .111	111 00	Not used	

Original Prefix
↑
Mask (VLAN) Mask 2 (Nodes) Mask 3 (Serial Links)

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-10

The figure shows an example of the calculation.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

VLSM:

- Provides the capability for route summarization to reduce required routing table entries and reduce CPU resources
- Helps an administrator maximize the number of IP addresses available (example: use of a /30 subnet mask on a point-to-point serial line using only two host addresses)
- Can calculate and use a hierarchical address plan by taking the number of addresses required plus two, then rounded up to the next higher power of two

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) Given the host address of 192.168.145.172/27, what is the range of addresses for this subnet?
- A) 192.168.145.128 through 192.168.145.191
 - B) 192.168.145.160 through 192.168.145.175
 - C) 192.168.145.160 through 192.168.145.191
 - D) 192.168.145.150 through 192.168.145.199
- Q2) Which three are benefits of using VLSM? (Choose three.)
- A) allows efficient use of IP address space
 - B) is supported by all classful and classless IP routing protocols
 - C) reduces the number of entries in the routing table
 - D) enables the creation of a hierarchical network design with route summarization

Quiz Answer Key

Q1) C

Relates to: Prefix Length and Network Mask

Q2) A, C, D

Relates to: Implementing VLSM in a Scalable Network

Route Summarization and Classless Interdomain Routing

Overview

As the result of corporate expansions and mergers, the number of subnets and network addresses in routing tables can increase rapidly. Route summarization and classless interdomain routing (CIDR) techniques can manage this corporate growth, much as Internet growth has been managed.

This lesson examines how route summarization uses VLSM. In VLSM, you break a block of addresses into smaller subnets. In route summarization, a group of subnets is rolled up into a summarized entry. In addition, this lesson demonstrates the technical similarities and differences between CIDR and route summarization.

Relevance

The size of most networks continues to grow. This growth taxes the CPU, memory, and bandwidth resources used to maintain the routing table. Route summarization has direct benefits for network performance. This concept applies directly to the advanced features found in scalable IP routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP), OSPF, Intermediate System-to-Intermediate System (IS-IS) Protocol, and Border Gateway Protocol (BGP). A thorough understanding of route summarization and CIDR makes it possible to implement a scalable network.

Objectives

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

- Describe route summarization implementation
- Calculate route summarization
- Explain CIDR

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- An understanding of IP subnetting, including complex subnetting and VLSM

Outline

The outline lists the topics included in this lesson.

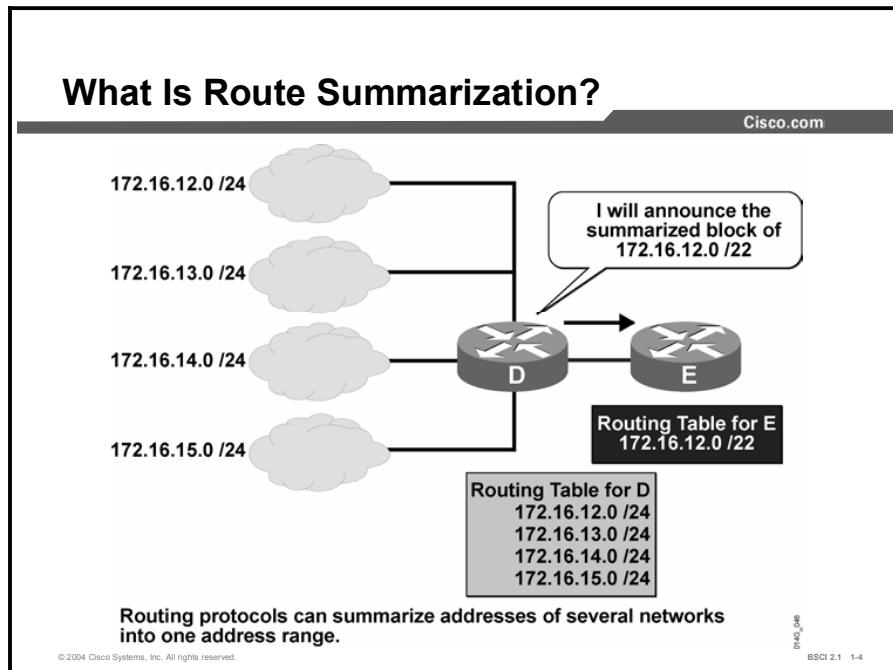
Outline

Cisco.com

- **Overview**
- **Route Summarization**
- **Calculating Route Summarization**
- **Classless Interdomain Routing**
- **Summary**
- **Quiz**

Route Summarization

This topic discusses route summarization and, by example, outlines the benefits of using route summarization to conserve address space.



Large internetworks must maintain hundreds, or even thousands, of network addresses. It is often problematic for routers to maintain this volume of network address routes in the routing tables. Route summarization, also known as route aggregation or supernetting, reduces the number of routes that a router must maintain by representing a series of network numbers in a single summary address.

In the figure, router D can send four routing update entries or summarize the addresses into a single network number. By summarizing the information into a single network number entry, router B maintains only one route and saves memory. Router D advertises this single route, which saves on bandwidth between routers D and E. Router E saves on CPU resources because it evaluates packets against fewer entries in the routing table.

Note In the example network, router D can route to network 172.16.12.0/22 and all subnets of that network. However, if there were other subnets of 172.16.12.0/22 elsewhere in the network (for example, if 172.16.15.0 were discontiguous), this summarization might not be valid.

Another advantage of using route summarization in a large, complex network is that it can isolate topology changes in one area of the network from other routers. That is, if a specific link (such as 172.16.13.0/24 in the example network) cycles up and down rapidly, the summary route (such as 172.16.12.0/22 in the example network) does not change on router E. Therefore, router E does not need to continually modify its routing table as the result of this flapping.

Note “Flapping” is a term commonly used to describe intermittent interface failure.

Route summarization is most effective within a subnetted environment when the network addresses are stored in contiguous blocks in powers of 2. For example, a single routing entry can represent 4, 6, or 512 addresses because summary masks are binary masks. Summarization must take place on binary boundaries (powers of 2), much like subnet masks.

Routing protocols summarize routes based on shared network numbers within the network. Classless routing protocols, such as Routing Information Protocol version 2 (RIPv2), OSPF, IS-IS, and EIGRP, support route summarization based on subnet addresses, including VLSM addressing. Classful routing protocols, such as Routing Information Protocol version 1 (RIPv1) and 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*.

Example

One way to understand the power of summarization is to imagine a company that operates a series of pizza shops, with 200 stores in every state in the United States. Each store has a router with an Ethernet and a Frame Relay link connected to headquarters. Without route summarization, the routing table on any of those routers would have 10,000 networks.

If each state has a central site to connect it with all the other states, and each of these routes is summarized before being announced to other states, then every router sees its local 200 subnets plus 49 summarized entries representing the other states. Which is less CPU-intensive: a routing table with 249 entries or one with 10,000 entries? Which uses less memory? Which uses less bandwidth to advertise its routing table?

Calculating Route Summarization

This topic demonstrates how to calculate route summarization.

Summarizing Within an Octet

Cisco.com

Common Bits = 22 Summary: 172.16.12.0 /22		Noncommon Bits = 10
172.16.11.0	10101100. 00010000.00001011.00000000	
172.16.12.0	10101100. 00010000.00001100.00000000	
172.16.13.0	10101100. 00010000.00001101.00000000	
172.16.14.0	10101100. 00010000.00001110.00000000	
172.16.15.0	10101100. 00010000.00001111.00000000	
172.16.15.255	10101100. 00010000.00001111.11111111	
172.16.16.0	10101100. 00010000.00010000.00000000	

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 1-5

The example router has the following networks in its routing table (you must summarize the networks before forwarding them):

- 172.16.12.0/24
- 172.16.13.0/24
- 172.16.14.0/24
- 172.16.15.0/24

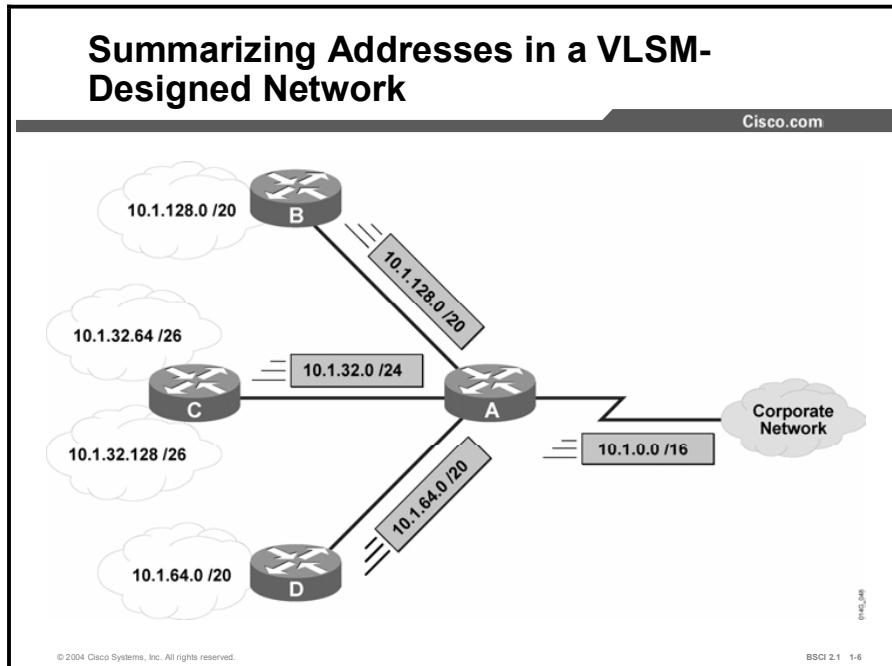
The summary route equates to the number of common bits shared among the IP addresses. To calculate the summary route, complete the following steps:

- Step 1** Find the number of highest-order bits that match in all the addresses, convert the addresses to binary format, and align them in a list.
- Step 2** Locate where the common pattern of digits ends. (It might be helpful to draw a vertical line marking the last matching bit in the common pattern.)
- Step 3** Count the number of common bits. This number is the summary route number. It is represented at the end of the first IP address in the block and preceded by a slash. In the figure, the first 22 bits of the IP addresses from 172.16.12.0 through 172.16.15.255 are the same. Therefore, the best summary route is 172.16.12.0/22.

Follow these guidelines to calculate route summarization:

- Addresses that do not share the same number of bits as the prefix length field of the summary route are not included in the summarization block. The IP addressing plan is hierarchical in nature to allow the router to aggregate the largest number of IP addresses into a single route summary. This approach is particularly important for VLSM use.
- An IP address can be summarized if the IP address number is a power of 2. If the address number is not a power of 2, you can divide the IP addresses into groups and summarize the groups separately.

Example



A VLSM design enables maximum use of IP addresses and more efficient routing update communication when hierarchical IP addressing is used. In the figure, route summarization occurs at the following two levels:

- Router C summarizes two routing updates from networks $10.1.32.64/26$ and $10.1.32.128/26$ into a single update: $10.1.32.0/24$.
- Router A receives three different routing updates; however, router A summarizes them into a single routing update before propagating it to the corporate network.

Route summarization reduces memory use on routers and reduces routing protocol network traffic. The following are the requirements for summarization to work correctly:

- 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.

Classless Interdomain Routing

This topic explains the purpose and benefits of implementing CIDR.

Classless Interdomain Routing

Cisco.com

- **CIDR is a mechanism developed to alleviate exhaustion of addresses and reduce routing table size.**
- **Block addresses can be summarized into single entries without regard to the classful boundary of the network number.**
- **Summarized blocks are installed in routing tables.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-7

CIDR alleviates IP address exhaustion and routing table growth. CIDR allows the combination of multiple address blocks with contiguous address space. This approach expands the set of IP addresses, regardless of whether the block violates the Class A, B, or C default network numbers in classful routing.

CIDR allocates blocks of network numbers to each network service provider. In addition, CIDR provides and subsets service provider address space to organizations that use the network service provider for Internet connectivity, when necessary.

Multiple contiguous blocks are summarized in routing tables, resulting in fewer route advertisements.

Note RFCs 1518 and 1519 further explain CIDR. RFC 2050, *Internet Registry IP Allocation Guidelines*, specifies guidelines for the allocation of IP addresses.

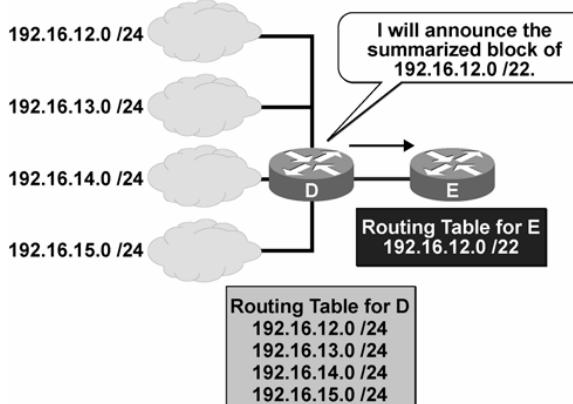
Most CIDR debates revolve around summarizing blocks of Class C networks into large blocks of addresses. As a general rule, Internet service providers (ISPs) implement a minimum route advertisement standard of /19 address blocks. (A /19 address block equals a block of 32 Class C networks.)

Addressing is now so limited that networks such as 12.0.0.0/8 are being divided into blocks of /19 that are assigned to major ISPs, which allows further allocation to customers.

CIDR combines blocks of addresses regardless of whether they fall within a single classful boundary or encompass many classful boundaries.

What Is CIDR?

Cisco.com



- Addresses are the same as in the route summarization figure, except that Class B network 172 has been replaced by Class C network 192.

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 1-8

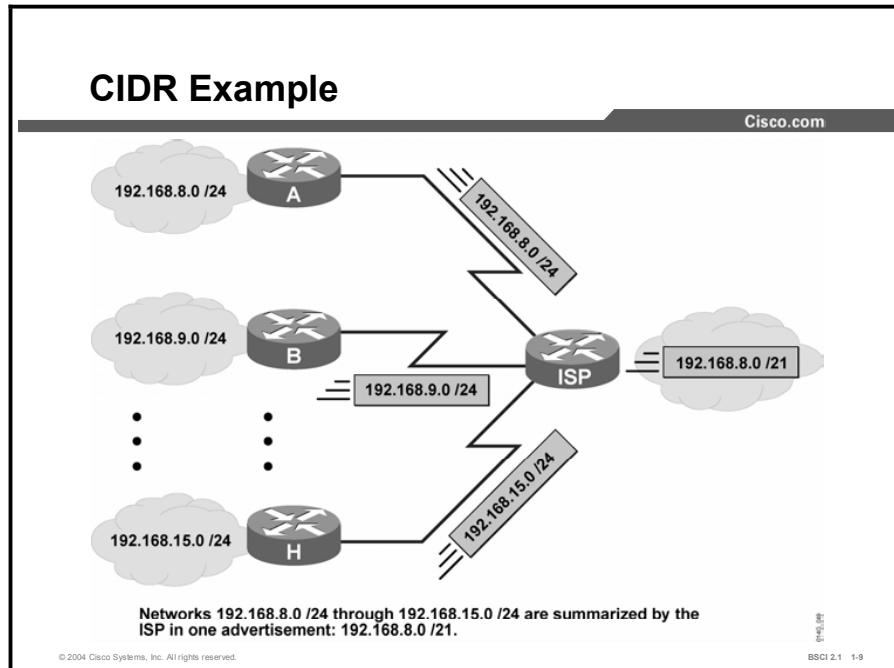
642_505

In this example, the ISP router (router D) uses and advertises the Class C network IP addresses 192.16.12.0/24 through 192.16.15.0/24. When the ISP router advertises the networks as available, it summarizes them into one route. It does not advertise the four Class C networks. The ISP router advertises 192.16.12.0/22 so that it can reach all destination addresses that have the first 22 bits the same as the first 22 bits of the address 192.16.12.0.

Note

The summary route number and CIDR route summary number both equate to the number of common bits shared among the IP addresses. To find the number of highest-order bits that match in all the addresses, convert the addresses to binary format and align them in a list. Locate where the common pattern of digits ends. (It is helpful to draw a vertical line marking the last matching bit in the common pattern.) Count the number of common bits. This number is the summary route number. It is represented at the end of the first IP address in the block and preceded by a slash. For example, the first 22 bits of the IP addresses from 192.16.12.0 through 192.16.15.255 are the same. Therefore, the best summary route is 192.16.12.0/22.

Example



In the figure, the first octet is 192, which identifies the networks as Class C networks. Combining these Class C networks into a block of addresses with a mask of less than /24 (the default Class C network mask), indicates that CIDR, not route summarization, is being performed. The difference between CIDR and route summarization is that route summarization is generally done within, or up to, a classful boundary, whereas CIDR combines several classful networks. In the figure, the eight separate 192.168.x.0 Class C networks that have the prefix /24 are combined into a single summarized block of 192.168.8.0/21. At some other point in the network, this summarized block can be further combined into 192.168.0.0/16.

Consider another example: A company that uses four Class B networks has the IP addresses 172.16.0.0/16 for Division A, 172.17.0.0/16 for Division B, 172.18.0.0/16 for Division C, and 172.19.0.0/16 for Division D. They can all be summarized as a single block: 172.16.0.0/14. This one entry represents the whole block of four Class B networks. This summarization process is CIDR; the summarization is going beyond the Class B boundaries.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Route summarization reduces the number of routes maintained by representing a series of networks as a single summary address**
- **Determine the summary route number by counting the number of common bits shared among the addresses of the networks to be summarized**
- **CIDR reduces IP address exhaustion by allowing combination of multiple address blocks that have contiguous address space but do not need to fall within a single classful boundary**

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 benefit is NOT a result of route summarization?
- A) Local topology changes are hidden from the routers to which the summarized route was announced.
 - B) Memory utilization is lowered.
 - C) Bandwidth use is reduced.
 - D) Details of all subnets in the internetwork are provided.
 - E) CPU usage is reduced.
- Q2) How can you summarize the IP range of addresses from 10.1.32.0 through 10.1.35.255?
- A) 10.1.32.0/23
 - B) 10.1.32.0/22
 - C) 10.1.32.0/21
 - D) 10.1.32.0/20
- Q3) You must summarize 192.168.12.0/24 and 192.168.13.0/24 into a single block. Which is the proper summarization and type of summarization for these networks?
- A) 192.168.12.0/23; route summarization
 - B) 192.168.12.0/23; CIDR
 - C) 192.168.12.0/22; CIDR
 - D) 192.168.12.0/22; route summarization

Quiz Answer Key

Q1) D

Relates to: Route Summarization

Q2) B

Relates to: Calculating Route Summarization

Q3) B

Relates to: Classless Interdomain Routing

Understanding IP Version 6

Overview

IP version 6 (IPv6) satisfies the increasingly complex requirements of hierarchical addressing that IP version 4 (IPv4) does not provide. Transitions to IPv6 from IPv4 deployments occur frequently. This lesson describes the functionality and benefits of IPv6. Cisco currently supports IPv6 in Cisco IOS Software Release 12.2(2)T and later.

Relevance

The ability to scale networks for future demands requires a new generation of IP addresses. IPv6 combines expanded addressing with a more efficient and feature-rich header to meet the demands for scalable networks in the future.

Objectives

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

- Identify the purpose and benefits of IPv6
- Describe IPv6 addressing
- List the fields in the header of an IPv6 address
- Explain how a 6to4 tunnel works

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Benefits of IP Version 6**
- **IPv6 Addressing**
- **IPv6 Frame Format**
- **IPv6-to-IPv4 Interoperability**
- **Summary**
- **Quiz**

Benefits of IP Version 6

This topic describes features and benefits of IPv6.

IPv6 Advanced Features

Cisco.com

- Larger address space:
 - Global reachability, flexibility
 - Aggregation
 - Multihoming
 - Autoconfiguration
 - Plug and play
 - Renumbering
- Simpler header:
 - Routing efficiency
 - Performance and forwarding rate scalability
 - Multicast rather than broadcast
 - No checksum calculation
 - Extension headers
 - Flow labels
- Mobility and security
 - Mobile IP RFC-compliant
 - IPSec a mandatory (or native) part of IPv6
- Transition richness
 - Dual stack
 - 6to4 tunnels
 - Translation

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI v2.1 1-4

IPv6 is a powerful enhancement to IPv4. The primary features of IPv6 are as follows:

- Larger address space provides new global reachability, flexibility, aggregation, multihoming, autoconfiguration, "plug and play," and renumbering.
- Simpler header enables better routing efficiency, performance, and forwarding rate scalability.
- Mobility and security ensure compliance with Mobile IP and IPSec standards functionality.
- Transition richness incorporates existing IPv4 capabilities with the added features of IPv6.

Mobility is an important feature in networks. Mobile IP is an Internet Engineering Task Force (IETF) standard available for both IPv4 and IPv6. The standard enables mobile devices to move without breaks in current connections. In IPv6, mobility is built in, which means that any IPv6 node can use it when necessary. However, mobility is not provided in IPv4; you must add it. The routing headers of IPv6 make mobile IPv6 much more efficient for end nodes than mobile IPv4.

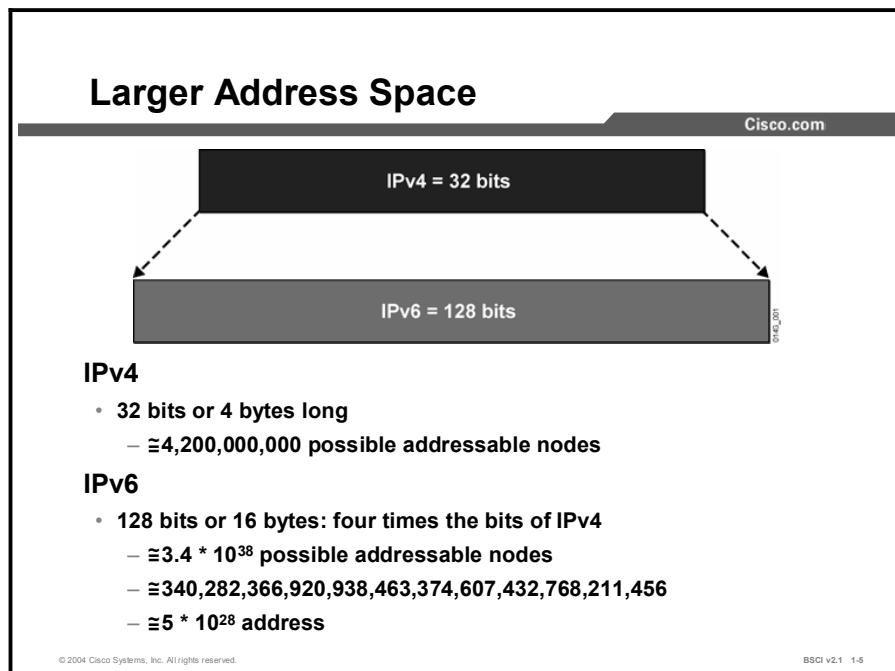
IPSec is the IETF standard for IP network security. It enables integrity, authentication, and confidentiality. IPSec is available for both IPv4 and IPv6. Although the functionalities are essentially identical in both environments, IPSec is mandatory in IPv6.

IPSec is enabled on every IPv6 node and is available for use. The availability of IPSec on all nodes makes the IPv6 Internet more secure. IPSec also requires keys for each party, which implies a global key deployment and distribution.

Note RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, defines the IPv6 standard.

IPv6 Addressing

This topic describes the features of IPv6 addressing.



IPv6 increases the number of address bits by a factor of 4, from 32 to 128. During the IPv6 design specification, factoring to 64, 128, and 160 bits was considered. Ultimately, the design team selected 128 bits as the most appropriate factoring choice. This factor enables a very large number of addressable nodes. However, as in any addressing scheme, there is a drawback: not all the addresses are used.

Increasing the number of bits for the address also increases the header size. Because each IP header contains a source and a destination address, the size of the header fields that contain the addresses is 64 bits for IPv4 and 256 bits for IPv6.

IPv6 Address Representation

Cisco.com

Format

- **x:x:x:x::x** where x is a 16-bit hexadecimal field
 - Case-insensitive
- **Leading zeros in a field are optional:**
 - 2031:0:130F:0:0:9C0:876A:130B
- **Successive fields of 0 are represented as ::, but only once in an address:**
 - 2031:0000:130F:0000:0000:09C0:876A:130B
 - 2031:0:130F::9C0:876A:130B
 - 2031::130F::9C0:876A:130B—incorrect
 - FF01:0:0:0:0:0:1 => FF01::1
 - 0:0:0:0:0:0:1 => ::1
 - 0:0:0:0:0:0:0 => ::

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-6

Colons separate entries in a series of 16-bit hexadecimal fields that represent IPv6 addresses. The A, B, C, D, E, and F in the hexadecimal fields are case-insensitive.

IPv6 does not require explicit address string notation. Use the following guidelines concerning IPv6 address string notations:

- The leading zeros in a field are optional, so that 09C0 = 9C0 and 0000 = 0.
- Successive fields of zeros can be represented as “::” only once in an address.
- An unspecified address is written as “::” because it contains only zeros.

Using the “::” notation greatly reduces the size of most addresses. For example, FF01:0:0:0:0:0:1 becomes FF01::1.

Note	An address parser identifies the number of missing zeros by separating the two parts and entering 0 until the 128 bits are complete. If two “::” notations are placed in the address, there is no way to identify the size of each block of zeros.
-------------	--

Multicast Use

Cisco.com

- **Broadcasts in IPv4**
 - Interrupt all computers on the LAN even if the intent of the request was for one or two computers
 - Can completely hang up a network (broadcast storm)
- **Broadcasts in IPv6**
 - Are not used; replaced by multicast and anycast
- **Multicast**
 - Enables efficient use of the network
 - Multicast address range much larger
- **Anycast**
 - Multiple devices share the same address
 - Source devices send packets to anycast address
 - Routers decide on closest device to reach that destination

©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-7

Broadcasting in IPv4 results in a number of problems. Broadcasting generates a number of interrupts in every computer on the network, and in some cases, completely halts an entire network. This event is known as a “broadcast storm.”

In IPv6, broadcasting does not exist. Broadcasts are replaced by multicasts and anycasts. Multicast enables efficient network operation by using a number of functionally specific multicast groups to send requests to a limited number of computers on the network. The multicast groups prevent the majority of problems related to broadcast storms in IPv4.

The range of multicast addresses in IPv6 is larger than in IPv4. For the foreseeable future, allocation of multicast groups is not being limited.

IPv6 defines a new type of address called an anycast address. The anycast address identifies a list of devices or nodes. You assign the same IPv6 unicast address to multiple devices that have a common function, such as the entry point to another autonomous system or the entry point to a distant subnet or network. You route a packet sent to an anycast address to the closest device or interface that shares this address. A sender creates a packet with the anycast as the destination address and forwards it to its nearest router. You send the anycast packet to the closest device or interface that the anycast address identifies according to the routing protocol. The source can use the anycast addresses to control the pathway across which traffic flows.

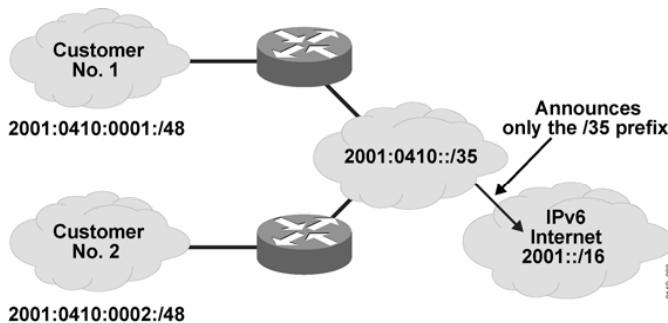
The unicast address space allocates the anycast addresses. To devices that are not configured for anycast, these addresses appear as unicast addresses. When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address.

An example of anycast use in a BGP multihomed network is when a customer has multiple ISPs with multiple connections to one another. You use a different anycast address for each ISP. Each router for that ISP has the same configured anycast address. The source device can choose which ISP to send the packet to. However, the routers along the path determine the closest router to reach that ISP using the anycast address.

Another use for an anycast is when a LAN is attached to multiple routers. These routers can have the same anycast address so that distant devices need to identify only the anycast address. Intermediate devices can choose the best pathway to reach the closest entry point to that subnet.

Address Aggregation

Cisco.com



Larger address space enables:

- Aggregation of prefixes announced in the global routing table
- Efficient and scalable routing

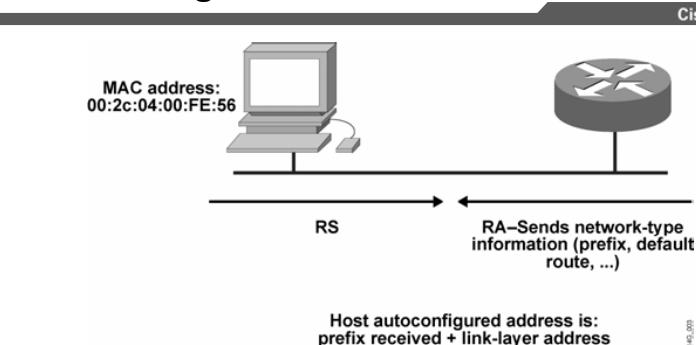
©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-8

Larger address spaces make room for large address allocations to ISPs and organizations. An ISP aggregates all the prefixes of its customers into a single prefix and announces the single prefix to the IPv6 Internet. The increased address space is sufficient to allow organizations to define a single prefix for the entire network as well.

Aggregation of customer prefixes results in an efficient and scalable routing table. Scalable routing is necessary to connect to various devices and networks on the Internet in the future.

Autoconfiguration



Larger address space enables:

- The use of link-layer addresses inside the address space
- Autoconfiguration with no duplicate addresses
- Plug and play

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-9

A much larger address space allows IPv6 engineers to design a better way to enable autoconfiguration of the addresses and maintain their global uniqueness. For example, a router on the local link sends network-type information, such as the prefix of the local link and the default route, to all its nodes. An IPv6-enabled host appends its 64-bit link-layer address to the 64-bit local link prefix to autoconfigure itself. This autoconfiguration produces a full 128-bit address that is usable on the local link and guarantees global uniqueness.

Note IPv6 detects duplicate addresses in special circumstances to avoid address collision.

Autoconfiguration enables plug and play, which connects devices (such as DHCP servers) to the network without configuration. Plug and play is a key feature to deploy new devices on the Internet, including cell phones, wireless devices, home appliances, and networks.

Autoconfiguration is accomplished via a handshake between the host and the router. The router sends a router advertisement (RA) immediately after the host sends a router solicitation (RS). The host sends an RS at boot time to request a router to send an immediate RA on the local link. The host then receives the autoconfiguration information without waiting for the next scheduled RA.

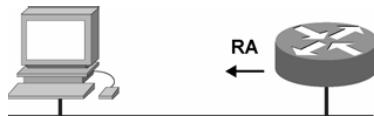
Routers also send RAs periodically, upon request, on all their configured interfaces. The router sends an RA to the “all nodes” multicast address. Information contained in the message includes:

- One or more prefixes to use on the link
- The lifetime of a prefix
- Flags that indicate the kind of autoconfiguration that hosts perform
- Default router information, including existence and lifetime
- Other types of host information

An RA sends prefixes to enable the autoconfiguration of hosts. The RA also assigns lifetimes to prefixes. Assigning prefixes enables the renumbering of hosts, because the lifetime of an old prefix decreases to zero and the new prefix has a normal lifetime. RA timing and other parameters can be configured on the routers.

IPv6 Renumbering

Cisco.com



RA packet definitions:

Src = Router link-local address

Dst = All-nodes multicast address

Data = Two prefixes:

Current prefix (to be deprecated) with short lifetime

New prefix (to be used) with normal lifetime

0162_004

Renumbering is achieved by modifying the RA to announce the old prefix with a short lifetime and the new prefix.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-10

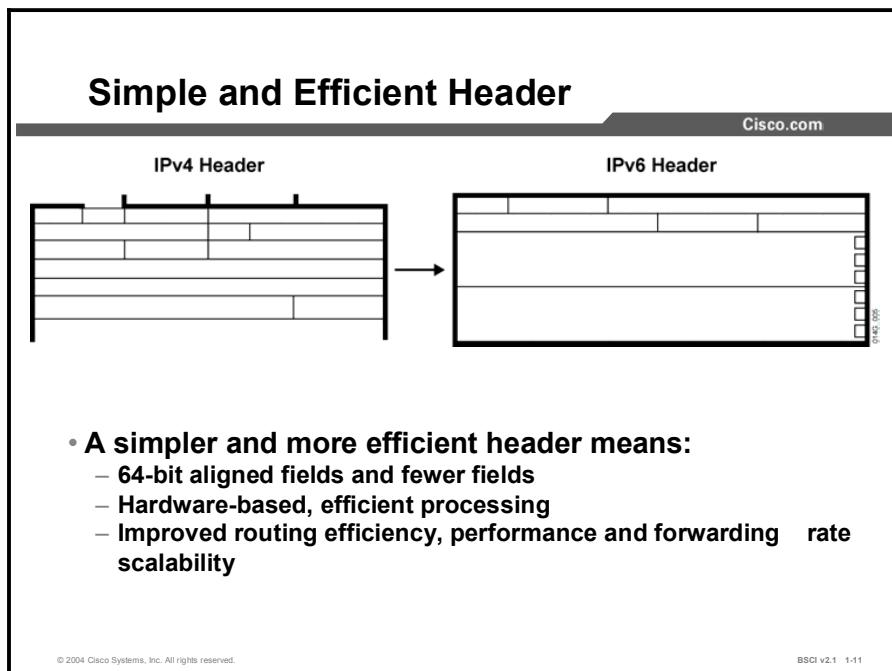
RAs are message transmissions that announce the pending retirement of an old node prefix and the use of a new node prefix. Decreasing the lifetime of the old prefix tells the nodes to begin using the new prefix and, at the same time, to continue maintaining connections opened with the old prefix. During that period, nodes have two unicast addresses that they can use. When the old node prefix is retired, the RA announces only the new node prefix.

If you do not use stateless autoconfiguration, use one of the other renumbering methods. Autoconfiguration greatly helps the renumbering process.

If you are renumbering an entire site, then you must also renumber the routers. A router renumbering protocol is currently under review by the IETF. When you renumber an entire site, you will need to make changes to the DNS entries. The introduction of new DNS records facilitates this process.

IPv6 Frame Format

This topic describes the IPv6 frame format.



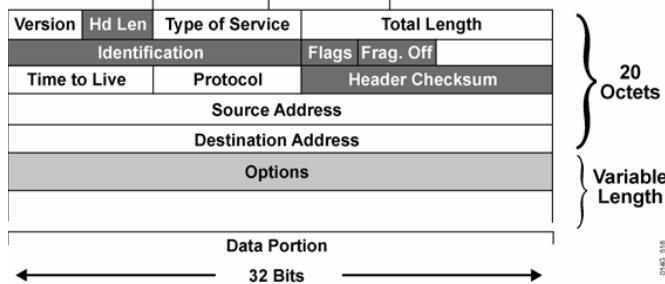
The new IPv6 header is less complicated than the IPv4 header in the following ways:

- It contains half of the previous IPv4 header fields. Fewer fields mean easier packet processing, enhanced performance, and routing efficiency.
- It enables direct routing data storage and faster routing data retrieval with 64-bit aligned fields.

IPv6 header enhancements enable hardware-based processing that provides forwarding-rate scalability for the next generation of high-speed lines. In the long term, it is clear that IPv6 improves routing efficiency. In the short term, however, the impact of the larger, 128-bit addressing remains unclear.

IPv4 Header Format

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-12

The IPv4 header contains 12 basic header fields, followed by an options field and a data portion (usually the transport-layer packet). The basic IPv4 header has a fixed size of 20 octets. The variable-length options field increases the size of the total IP header.

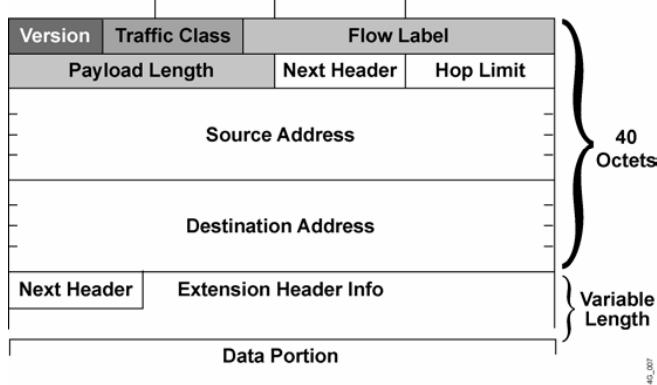
IPv6 contains 5 of the 12 IPv4 basic header fields. The IPv6 header does not require the other 7 fields for the following reasons:

- Routers handle fragmentation in IPv4, which causes a variety of processing issues. IPv6 routers no longer perform fragmentation. Instead, a discovery process is used to determine the most optimum maximum transmission unit (MTU) to use during a given session.
 - In the discovery process, the source IPv6 device attempts to send a packet at the size specified by the upper IP layers, for example, the transport and application layers. If the device receives an “ICMP packet too big” message, it informs the upper layer to discard the packet and to use the new MTU. The “ICMP packet too big” message contains the proper MTU size for the pathway. Each source device needs to track the MTU size for each session. Generally, the tracking is done by creating a cache based on the destination address; however, it also can be done by using the flow label. If source-based routing is performed, the tracking of the MTU size can be done by using the source address.
 - The discovery process is beneficial because as routing pathways change, a new MTU can be more appropriate. When a device receives an “ICMP packet too big” message, it decreases its MTU size if the ICMP message contains a recommended MTU less than the current MTU of the device. A device can perform an MTU discovery every 5 minutes to see if the MTU has increased along the pathway.
 - Application and transport layers for IPv6 accept MTU reduction notifications from the IPv6 layer. If they do not, IPv6 has a mechanism to fragment packets that are too large. However, upper layers are encouraged to avoid sending messages that require fragmentation.

- Most currently implemented link-layer technologies already do checksum and error control. Because link-layer technologies are relatively reliable, an IP header checksum is considered to be redundant. Without the IP header checksum, the upper-layer optional checksums, such as UDP, are now mandatory.

IPv6 Header Format

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 - 1-13

The IPv6 header has 40 octets in contrast to the 20 octets in IPv4. IPv6 has a smaller number of fields, and the header is 64-bit aligned to enable fast processing by current processors. Address fields are four times larger than in IPv4.

The IPv6 header contains these fields:

- **Version:** A 4-bit field, the same as in IPv4. It contains the number 6 instead of the number 4 for IPv4.
- **Traffic class:** An 8-bit field similar to the type of service (ToS) field in IPv4. It tags the packet with a traffic class that it uses in differentiated services. These functionalities are the same for IPv6 and IPv4.
- **Flow label:** A completely new 20-bit field. It tags a flow for the IP packets. It can be used for multilayer switching techniques and faster packet-switching performance.
- **Payload length:** Similar to the total length field of IPv4.
- **Next header:** The value of this field determines the type of information following the basic IPv6 header. It can be a transport-layer packet, such as TCP or UDP, or it can be an extension header, as shown in the graphic. The next header field is similar to the protocol field of IPv4.

IPv6 also uses the Stream Control Transmission Protocol (SCTP) at the transport layer. SCTP is a reliable transport service like TCP and supports sequence and acknowledgement functions. SCTP was designed to overcome some limitations of TCP, for example, the TCP requirement for a strict order of transmission that can cause head-of-line blocking.

The main difference between the two protocols lies in the purpose of SCTP. SCTP is used for multihomed nodes and for combining several streams within a single data connection. TCP sends a stream of bytes, while SCTP sends a stream of messages. In TCP, the application has to know how to divide the stream of bytes into usable segments. SCTP is designed to provide a general-purpose transport protocol for message-oriented applications, such as the signaling used in the public telephone network. If multiple streams are integrated into one connection and

one of these streams has reliability problems, then all the streams in TCP have difficulty. SCTP is aware of the messages in the connection, and functionality is provided with SCTP to selectively acknowledge SCTP packets.

In multihoming, clients and servers can have multiple network interface cards (NICs), and each can be reached by a variety of different physical pathways. During SCTP setup, the client informs the server of all its IP addresses. The client needs to know a single address only for the server, because when the server responds to the client, it has in its acknowledgment a list of addresses to use to reach it. SCTP monitors all pathways between the devices with a heartbeat function and identifies one pathway as the primary. You can use secondary pathways for retransmissions or in case the primary pathway fails.

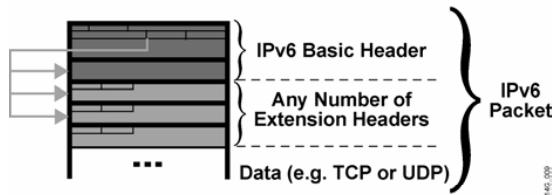
SCTP has greater security than TCP, because SCTP uses a cookie function for each session and is immune to a TCP SYN attack.

- **Hop limit:** This field specifies the maximum number of hops that an IP packet can traverse. Each hop or router decreases this field by one. Since there is no checksum in the IPv6 header, the router can decrease the field without recomputing the checksum. On IPv4 routers the recomputation costs processing time.
- **Source address:** This field has 16 octets or 128 bits. It identifies the source of the packet.
- **Destination address:** This field has 16 octets or 128 bits. It identifies the destination of the packet.

The extension headers, if any, and the data portion of the packet follow the eight fields. The number of extension headers is not fixed, so the total length of the extension header chain is variable.

IPv6 Extension Headers

Cisco.com



- **Simpler and more efficient header means:**
 - IPv6 has extension headers
 - It handles the options more efficiently
 - It enables faster forwarding rate and end nodes processing

©2004 Cisco Systems, Inc. All rights reserved.

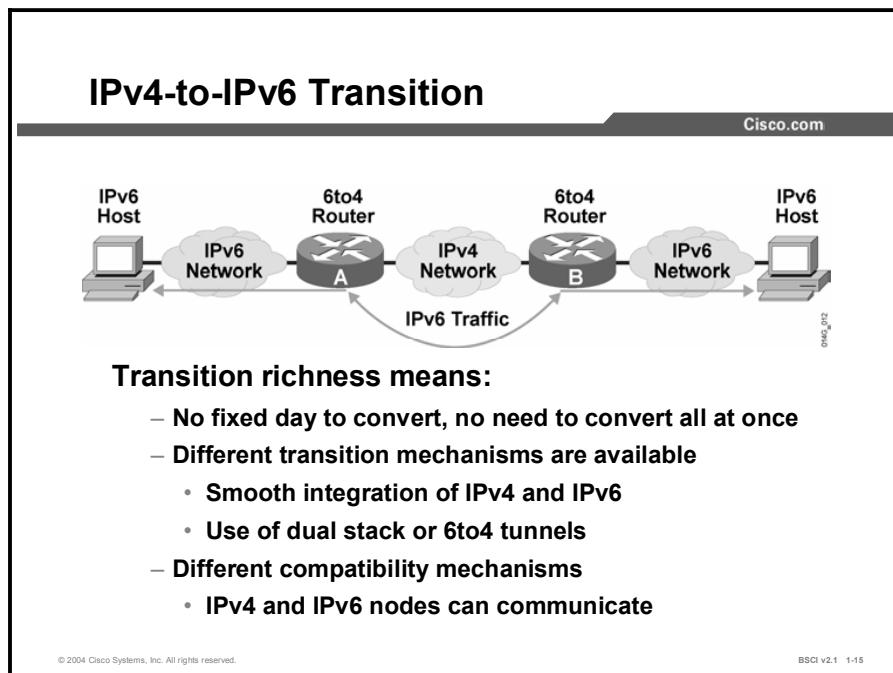
BSCI v2.1 1-14

There are many types of extension headers. When multiple extension headers are used in the same packet, the order of the headers should be:

1. IPv6 header
2. Hop-by-hop options header
3. Destination options header (when using the routing header)
4. Routing header
5. Fragment header
6. Authentication header
7. Encapsulating Security Payload (ESP) header
8. Destination options header
9. Upper-layer header

IPv6-to-IPv4 Interoperability

This topic describes the process for making the transition from IPv4 to IPv6.



The transition from IPv4 does not require upgrades on all nodes at the same time. Many transition mechanisms enable smooth integration of IPv4 and IPv6. Other mechanisms that allow IPv4 nodes to communicate with IPv6 nodes are available. All these mechanisms are applied to different situations.

The two most common techniques to transition from IPv4 to IPv6 are:

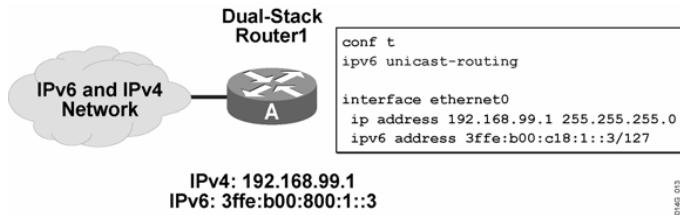
- Dual stack
- IPv6-to-IPv4 (6to4) tunnels

A third method is to use an extension of IP NAT to translate the IPv4 address to an IPv6 address and IPv6 to IPv4.

The figure shows an example of a transition and integration mechanism. The 6to4 routers automatically encapsulate the IPv6 traffic inside IPv4 packets.

Cisco IOS Dual Stack

Cisco.com



d145_013

Cisco IOS is IPv6-ready:

If both IPv4 and IPv6 are configured on an interface, this interface is dual-stacked.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-16

Cisco IOS software is IPv6-ready. As soon as IPv4 and IPv6 basic configurations are complete on the interface, the interface is dual-stacked, and it forwards IPv4 and IPv6 traffic.

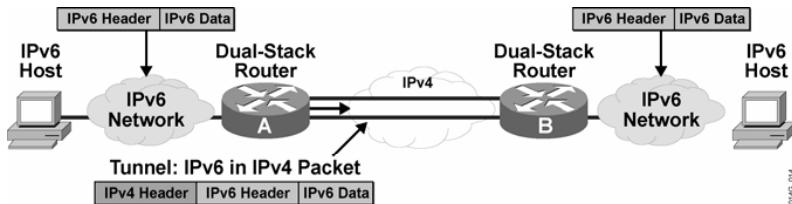
Using IPv6 on a Cisco IOS router requires that you use the global configuration command **ipv6 unicast routing**. This command enables the forwarding of IPv6 datagrams. All interfaces that forward IPv6 traffic must have an IPv6 address. The interface command is:

ipv6 address IPv6-address [/prefix length]

This command specifies an IPv6 network assigned to the interface and enables IPv6 processing on the interface.

Overlay Tunnels

Cisco.com



Tunneling encapsulates the IPv6 packet in the IPv4 packet.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-17

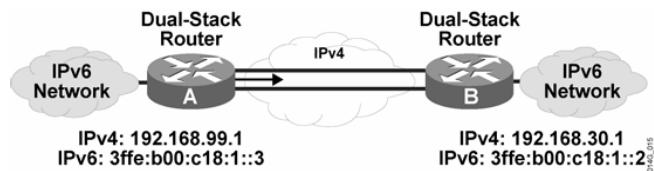
Networking often uses tunnels to overlay an incompatible functionality over an existing network. Tunneling IPv6 traffic over an IPv4 network requires one edge router to encapsulate the IPv6 packet inside an IPv4 packet and another router to de-encapsulate it. This process enables you to connect the IPv6 islands without converting the entire network to IPv6.

When you tunnel, remember the following two issues:

- If the IPv4 header does not contain an optional field, the MTU effectively decreases by 20 octets.
- A tunneled network is often difficult to troubleshoot. Tunneling is a transition technique that should be used only where it is appropriate; do not consider it a final architecture. Native IPv6 architecture is still the target architecture.

Configured Tunnel

Cisco.com



- **Configured tunnels require:**
 - Dual-stack endpoints
 - IPv4 and IPv6 addresses configured at each end

©2004 Cisco Systems, Inc. All rights reserved.

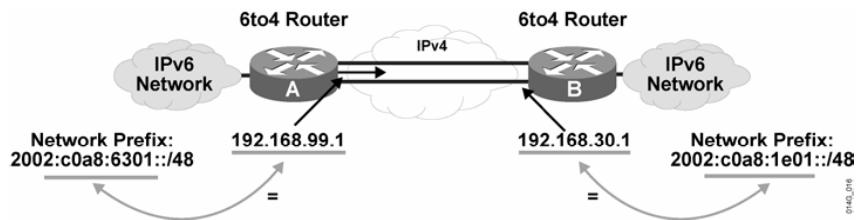
BSCI v2.1 1-18

In a manually configured tunnel, you configure both the IPv4 and IPv6 addresses statically. Perform this configuration on the routers at each end of the tunnel. These end routers must be dual-stacked, and the configuration cannot change dynamically as network and routing needs change. Routing must be set up properly to forward a packet between the two IPv6 networks.

Tunnel endpoints can be unnumbered, but unnumbered endpoints make troubleshooting difficult. The IPv4 practice of saving addresses for tunnel endpoints is no longer an issue.

6to4 Tunneling

Cisco.com



- **6to4:**
 - Is an automatic tunnel method
 - Gives a prefix to the attached IPv6 network

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-19

The 6to4 tunneling method automatically establishes the connection of IPv6 islands through an IPv4 network. The 6to4 tunneling method applies a valid IPv6 prefix to each IPv6 island, which enables the fast deployment of IPv6 in a corporate network without address retrieval from the ISPs or registries.

The 6to4 tunneling method requires a special code on the edge routers, but the IPv6 hosts and routers inside the 6to4 site do not require new features to support 6to4. Each 6to4 site receives a /48 prefix, which is the concatenation of 2002 and the IPv4 address of the edge router.

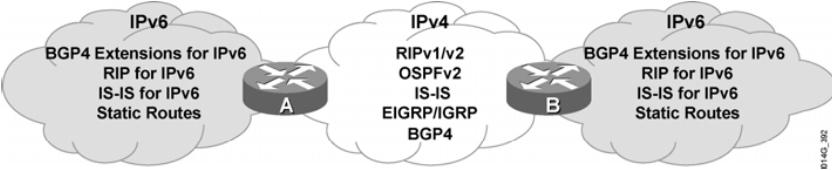
For example, if the IPv4 address of the edge router is 192.168.99.1, the prefix of its IPv6 network is 2002:c0a8:6301::/48, because c0a86301 is the hexadecimal representation of 192.168.99.1. The IPv6 network can substitute any IP address in the space after the first 16-bit section (0x2002).

When an IPv6 packet with a destination address in the range of 2002::/16 reaches the 6to4 edge router, the 6to4 edge router extracts the IPv4 address embedded in the 2002:: destination address (inserted between the third and sixth octets inclusively). The 6to4 router then encapsulates the IPv6 packet in an IPv4 packet with the destination IPv4 address extracted from inside the IPv6 destination address. This IPv4 address represents the address of the other 6to4 edge router of the destination 6to4 site. The destination edge router de-encapsulates the IPv6 packet in the IPv4 packet and then forwards the native packet toward its final destination.

Note 2002::/16 is the address range specifically assigned to 6to4.

IPv6 Routing Protocols

Cisco.com



B140-302

IP routing protocols supporting IPv6 and their Cisco IOS release:

- Integrated IS-IS for IPv6 Release 12.0(22)S and 12.2(8)T
- BGP extensions for IPv6 Release 12.0(22)S and 12.2(2)T
- RIP for IPv6 Release 12.0(22)S and 12.2(2)T
- Static routes—Release 12.0(22)S and 12.2(2)T

©2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-28

If the IPv6 clouds in either a 6to4 tunnel or a dual stack have multiple IPv6 routers, then an IPv6 routing protocol must be enabled on those routers. In the Cisco 12000 Series Internet router, IPv6 routing is supported in the Cisco IOS Software Release 12.0(22)S configuration and later. In all other platforms, the IPv6 routing protocols are supported in Cisco IOS Release 12.2(2)T and later. If multiple IPv6 routing protocols are used, only the listed IPv6 protocols in the figure support redistribution. Redistribution is not supported between IPv4 routing protocols and IPv6 routing protocols.

The largest use of IPv6 is across the Internet, using BGP extensions for IPv6.

OSPF version 3 supports IPv6 and is part of the Cisco IOS software released at the end of 2002 as part of the Cisco IOS software IPv6 Phase III implementation.

Cisco EIGRP for IPv6 is also part of the Cisco IOS software released at the end of 2002. EIGRP for IPv6 is also part of the Cisco IOS software IPv6 Phase III implementation.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- The new address space is the most significant feature of IPv6. The address has been increased from 32 bits in IPv4 to 128 bits in IPv6.
- Also important to IPv6 is the new header format—64-bit alignment means faster processing speeds for packets. Unnecessary fields have been removed, and a new extension header has been added for optional fields.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-21

Summary (Cont.)

Cisco.com

- IP address numbering and renumbering issues have been solved through a new autoconfiguration technique. This scheme will eliminate the need for DHCP and manual IP addressing.
- Security and mobility are built into the specification.
- Making the transition from an IPv4 network to an IPv6 network is complex. However, making the transition schemes have been carefully considered. Two of the most common are dual stack and 6to4 tunneling.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI v2.1 1-22

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 only difference between IPv6 and IPv4 headers is the address format.

- A) true
- B) false

Q2) What three features does an extended address space will provide: (List three features.)

- A) _____
- B) _____
- C) _____

Q3) The IPv6 header will have a 128-bit addressing format. How many bytes is 128 bits?

- A) 4
- B) 8
- C) 16
- D) 32

Q4) Write out the following address completely. Make sure that you include all bytes.

2101:0:A::45:1234

Q5) While IPv4 uses /prefix notation to describe address aggregation blocks, IPv6 will not use this technique.

- A) true
- B) false

Q6) In the autoconfiguration technique of IPv6, a client station will automatically learn its network address. Which part of the address is sent from the router to the host?

- A) MAC address
- B) network prefix
- C) entire network address

Q7) A host address is made up of a network prefix, sent by the router, plus the Layer 2 address of the host.

- A) true
- B) false

Q8) If an IPv4 header is typically 20 bytes long, how long will an IPv6 header be (assuming no Option fields)?

- A) 20 bytes as well
- B) 40 bytes
- C) 60 bytes
- D) 80 bytes

Q9) The IPv6 header does not use several of the IPv4 fields.
Name two fields no longer defined in the IPv6 header.

- A) _____
- B) _____

Q10) An IPv6 header is 32-bit aligned for faster CPU processing.

- A) true
- B) false

Q11) Name two transition strategies from IPv4 to IPv6.

- A) _____
- B) _____

Q12) Define a dual-stack approach.

Q13) Which two features are advantages of a 6to4 tunnel? (Choose two.)

- A) The tunnel must be manually configured.
- B) The tunnel is automatically established on demand.
- C) The IPv4-formatted packet rides inside an IPv6-packet.
- D) The IPv6-formatted packet rides inside an IPv4-packet.

Quiz Answer Key

Q1) B

Relates to: Benefits of IP Version 6

Q2) global reachability
aggregation
autoconfiguration

Relates to: Benefits of IP Version 6

Q3) C

Relates to: IPv6 Addressing

Q4) 2101:0000:000A:0000:0000:0000:0045:1234

Relates to: IPv6 Addressing

Q5) B

Relates to: IPv6 Addressing

Q6) B

Relates to: IPv6 Addressing

Q7) A

Relates to: IPv6 Addressing

Q8) B

Relates to: IPv6 Frame Format

Q9)

Fragmentation
header checksum

Relates to: IPv6 Frame Format

Q10)

B

Relates to: IPv6 Frame Format

Q11)

dual stack
6to4 tunnel, manual tunnel

Relates to: IPv6-to-IPv4 Interoperability

Q12)

Dual stack means that a router interface has both an IPv4 and an IPv6 address defined simultaneously. This allows the router interface to support both formats so that a packet from either format can be routed.

Relates to: IPv6-to-IPv4 Interoperability

Q13)

B, D

Relates to: IPv6-to-IPv4 Interoperability

Network Address Translation

Overview

Network Address Translation (NAT) is an important function in most scalable networks. NAT is mandatory for the majority of companies that have Internet connections. ISPs have hundreds of users accessing the Internet, yet commonly they are assigned only 8 or 16 individual addresses. The ISPs use NAT to map the hundreds of inside addresses to the few globally unique addresses assigned to that company. This lesson demonstrates by example:

- How to use basic NAT and a standard access list to assign separate address space to different users.
- How to use an extended access list to check the destination address of a packet and assign different source addresses based on the destination address of the packet.
- How to use a Cisco IOS software tool called a *route map* to create a fully extended address translation in an IP NAT table. The IP NAT table tracks the original address and its translation as well as the destination address and the TCP and User Datagram Protocol (UDP) ports for each.

Relevance

Corporations use NAT in a variety of ways. Troubleshooting a network translation router is often complicated and time-consuming. In practice, configuring basic NAT, setting up alternate address pools for different groups of users, and creating fully extended translation tables enhances and simplifies troubleshooting tasks.

Objectives

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

- Configure IP NAT for multiple address pools using access lists
- Identify the results of using a route map for NAT
- Explain the basic structure of a route map
- Describe the commands to configure NAT with route maps

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- An understanding of filtering traffic with standard and extended access lists

Outline

The outline lists the topics included in this lesson.

Outline

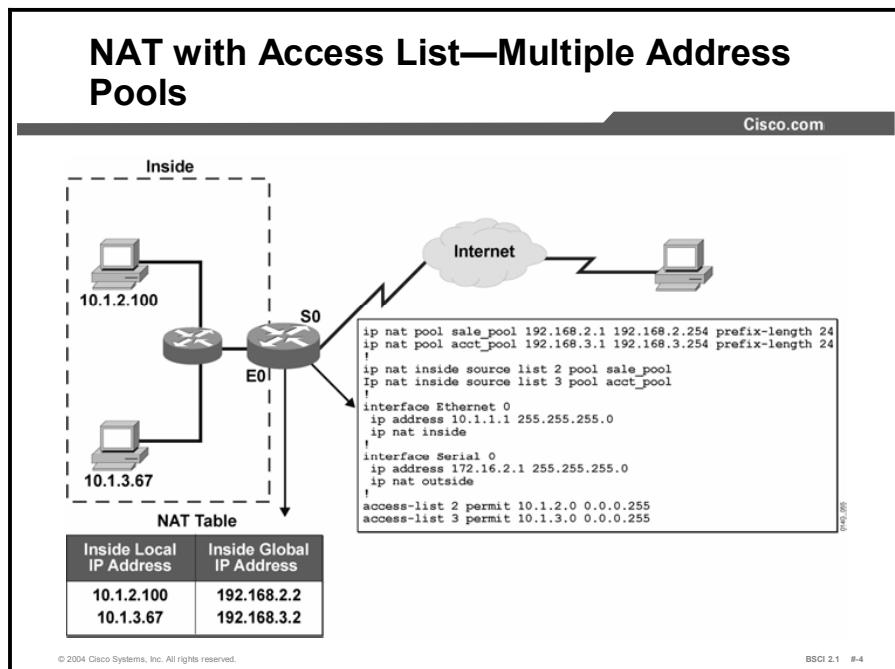
Cisco.com

- Overview
- Configuring IP NAT with Access Lists
- Defining the Route Map Tool for NAT
- Using Basic route-map Commands
- Configuring IP NAT with Route Maps
- Summary
- Quiz

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 #3

Configuring IP NAT with Access Lists

This topic explains the IP NAT commands to configure IP NAT with access lists. It provides a sample IP NAT configuration and two specific examples to configure IP NAT with access lists. The first example demonstrates how to use access lists to qualify whether an IP address needs translation based on the original source address. The second example demonstrates how to use an access list to assign a NAT source IP address based on the source and destination addresses of the original packet.



Following is NAT-related terminology for interfaces that exist inside and outside networks:

- **IP NAT inside:** Interfaces that are part of the network address space inside the company and that have the set of networks that are subject to translation
- **IP NAT outside:** Interfaces connected to routers that are outside the corporate network or that do not carry the IP NAT inside address space in their routing tables

NAT is performed when a packet is routed between the following interfaces:

- An IP NAT inside interface to an IP NAT outside interface
- An IP NAT outside interface to an IP NAT inside interface

NAT builds an entry in the IP NAT table as the packet goes from an IP NAT inside interface. A NAT entry usually changes the source IP address from an inside address to an outside address. When an IP NAT outside interface responds to the packet, the destination IP address of the returning packet is compared to the entries in the IP NAT table.

If a match is found, the destination IP address is translated to the correct inside address and sent to the routing table to be routed to the correct IP NAT inside interface. If no match is found, the packet is discarded.

Address overloading is a common occurrence in many Internet connections. Overloading occurs when many inside addresses are mapped to one or a few globally unique addresses using NAT. NAT includes TCP and UDP ports in the mapping process to uniquely identify each session.

When the router determines that the path of a packet is from an IP NAT inside interface to an IP NAT outside interface, an entry is created to include both the original source IP address and the original TCP for UDP port number.

Each of these devices is assigned a unique TCP or UDP source port number to distinguish it from the others. When a packet returns to the IP NAT outside interface, it is compared to the IP NAT table. Although the packet destination address could match thousands of entries, NAT checks the destination TCP or UDP port for the correct entry for the returning packet. Once the correct entry is found, the current destination address and port number change to the appropriate IP NAT inside destination address and port number.

A NAT table contains the following information:

- **Protocol:** Either IP, TCP, or UDP.
- **Inside local IP address: Port**—The IP address of an inside host before any translations. The inside local IP address is usually the private addressing found in RFC 1918.
- **Inside global IP address: Port**—The IP address of an inside host as it appears to the outside network, or the translated IP address. Addresses are allocated from a globally unique address space, typically provided by the ISP if the enterprise connects to the global Internet.
- **Outside global IP address: Port**—The configured ISP IP address assigned to a host in the outside network.
- **Outside local IP address: Port**—The IP address of an outside host as it appears to the inside network. Outside local IP addresses can be allocated from the RFC 1918 space, if desired.

The following commands are used to configure IP NAT with access lists:

- **ip nat {inside | outside}:** This interface command marks the IP devices behind that interface as either internal or external to the controlled network. Only packets arriving on an interface marked as IP NAT inside or outside are subject to translation.
- **ip nat inside source list <access-list number> pool <address_pool_name>:** When a packet comes in on an interface marked as IP NAT inside, this command informs the router to compare the source IP address to the access list number in the command. Then the access list tells the router whether or not to translate that source IP address to the next available address in the address pool name listed. An address that is permitted in the access list will be translated by NAT.
- **ip nat pool <address_pool_name> <starting_ip_address> <ending_ip_address> {prefix-length <prefix-length> | netmask <netmask>}:** This command creates the translation pool by assigning the same name to the IP NAT pool as the **ip nat inside source list <access-list-number> pool** command. The command needs to include the starting and ending addresses for translation and either the prefix length or network mask associated with this range of addresses.

In the preceding figure, when an IP packet comes in on Ethernet 0 and has a source address of 10.1.2.x, the router translates it from the NAT pool of addresses defined by the name sale_pool.

If the packet has a source address of 10.1.3.x, the router translates it from the NAT pool of addresses defined by the name acct_pool.

Use the configuration from the figure if your company needs to map groups of users to different blocks of NAT addresses. Information services departments can determine what percentage of users per division or department use the interface that is configured with NAT. (The percentage of users is typically determined using accounting or security software for the charge-back system.)

Example

NAT with Extended Access List Configuration

Cisco.com

```
ip nat pool trusted_pool 192.168.2.1 192.168.2.254 prefix-length 24
ip nat pool untrusted_pool 192.168.3.1 192.168.3.254 prefix-length 24
!
ip nat inside source list 102 pool trusted_pool
ip nat inside source list 103 pool untrusted_pool
!
interface ethernet 0
 ip address 10.1.1.1 255.255.0.0
 ip nat inside
!
interface serial 0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 permit ip 10.1.1.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 103 permit ip 10.1.1.0 0.0.0.255 any
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 #5

In this configuration example of NAT, the extended access lists 102 and 103 are used to control NAT decisions. Instead of making the decision based only on the source address, an extended access list makes the decision based on the source and destination addresses of all packets coming in on interface Ethernet 0.

If the packet is not from the 10.1.1.0/24 subnet, the source IP address of the packet is not translated. If the packet is from the 10.1.1.0/24 subnet and the destination address matches either part of 172.16.1.0/24 or 192.168.200.0/24, the source IP address is translated to the next available address in the trusted pool, which is the 192.168.2.0/24 network.

If the packet is from the 10.1.1.0/24 subnet and the destination address does not match either 172.16.1.0/24 or 192.168.200.0/24, the source IP address is translated to the next available address in the untrusted pool, which is the 192.168.3.0/24 network.

Use the type of configuration in the figure only if the outside NAT environment has both trusted and untrusted sites. The company can be attached to an industry internetwork where it exchanges information with corporate partners and competitors. The 172.16.1.0/24 and the 192.168.200.0/24 can be addresses of trusted networks on the industry internetwork, but all other destination addresses are considered untrusted. You can configure the firewall system to allow greater latitude to the trusted sites to determine what they can access and the applications that they can use.

Defining the Route Map Tool for NAT

A route map is a Cisco IOS software function that serves a variety of purposes. This topic explains the route map tool and compares the results of using a route map tool to the results of using only an access list with NAT.

Benefits of Route Maps with NAT																															
Cisco.com																															
NAT Table with Access List Only																															
<table border="1"><thead><tr><th>Protocol</th><th>Inside Local IP Address: Port</th><th>Inside Global IP Address: Port</th><th>Outside Global IP Address: Port</th></tr></thead><tbody><tr><td>—</td><td>10.1.1.1</td><td>192.168.2.1</td><td>—</td></tr><tr><td>—</td><td>10.1.1.2</td><td>192.168.3.1</td><td>—</td></tr><tr><td>—</td><td>10.1.1.3</td><td>192.168.2.2</td><td>—</td></tr></tbody></table>				Protocol	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port	—	10.1.1.1	192.168.2.1	—	—	10.1.1.2	192.168.3.1	—	—	10.1.1.3	192.168.2.2	—												
Protocol	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port																												
—	10.1.1.1	192.168.2.1	—																												
—	10.1.1.2	192.168.3.1	—																												
—	10.1.1.3	192.168.2.2	—																												
NAT Table Using Route Maps and Access Lists																															
<table border="1"><thead><tr><th>Protocol</th><th>Inside Local IP Address: Port</th><th>Inside Global IP Address: Port</th><th>Outside Global IP Address: Port</th></tr></thead><tbody><tr><td>UDP</td><td>10.1.1.1:1024</td><td>192.168.2.1:1024</td><td>172.16.1.20:69</td></tr><tr><td>TCP</td><td>10.1.1.1:4097</td><td>192.168.2.1:4097</td><td>172.16.1.20:21</td></tr><tr><td>TCP</td><td>10.1.1.1:1084</td><td>192.168.2.1:1084</td><td>172.16.1.20:20</td></tr><tr><td>TCP</td><td>10.1.1.2:1024</td><td>192.168.3.1:1024</td><td>172.20.7.3:80</td></tr><tr><td>TCP</td><td>10.1.1.3:5553</td><td>192.168.2.2:5553</td><td>192.168.200.25:23</td></tr><tr><td>TCP</td><td>10.1.1.3:5554</td><td>192.168.2.2:5554</td><td>192.168.200.25:80</td></tr></tbody></table>				Protocol	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port	UDP	10.1.1.1:1024	192.168.2.1:1024	172.16.1.20:69	TCP	10.1.1.1:4097	192.168.2.1:4097	172.16.1.20:21	TCP	10.1.1.1:1084	192.168.2.1:1084	172.16.1.20:20	TCP	10.1.1.2:1024	192.168.3.1:1024	172.20.7.3:80	TCP	10.1.1.3:5553	192.168.2.2:5553	192.168.200.25:23	TCP	10.1.1.3:5554	192.168.2.2:5554	192.168.200.25:80
Protocol	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port																												
UDP	10.1.1.1:1024	192.168.2.1:1024	172.16.1.20:69																												
TCP	10.1.1.1:4097	192.168.2.1:4097	172.16.1.20:21																												
TCP	10.1.1.1:1084	192.168.2.1:1084	172.16.1.20:20																												
TCP	10.1.1.2:1024	192.168.3.1:1024	172.20.7.3:80																												
TCP	10.1.1.3:5553	192.168.2.2:5553	192.168.200.25:23																												
TCP	10.1.1.3:5554	192.168.2.2:5554	192.168.200.25:80																												
<small>© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 B-6 0140_08</small>																															

When you use only access lists for NAT, the result is the ability to identify only which inside local address is being translated to which inside global address. One-for-one NAT mapping and an access list provide a simple translation entry, as shown in the top part of the figure. The simple translation entry contains local and global IP address entries for only the inside translation and does not include any TCP or UDP port information or the destination address of an outbound packet.

The entries in the IP NAT translation table are called simple entries because they track only the original source address (inside local) and the address to which it is translated (inside global). The other fields are left blank. It is difficult to troubleshoot connectivity using simple NAT translations because you do not see the destination address or the application associated with each NAT translation. This inability to see destination address or associated application also prevents proper translation among multiple address pools. The first address pool matched creates a simple NAT entry. A second session initiated to a different host already matches the simple entry, thereby preventing proper translation to the second address pool.

To get a fully extended translation entry, you need to configure NAT for overloading or use a Cisco IOS software tool called a route map. If you configure a route map to use in conjunction with an access list for NAT, it generates an extended translation entry, as shown in the bottom part of the figure. The extended translation entry identifies the source and destination addresses with the appropriate translation, that transport layer that is used, and the port or application that is used throughout the session. The extended translation entry also contains the local and global address entries.

Route Maps

Cisco.com

Route maps are complex access lists:

- Lines in access lists ⇒ statements in route maps
- Access list number ⇒ route map name
- Addresses and masks in access lists ⇒ match statements in route maps
- Statements in route map can be optionally numbered
- Route map statements can modify matched route with set command

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 #7

Route maps are complex access lists that allow conditions to be tested against a packet or route using **match** commands. If the conditions match, specific actions are taken to modify attributes of the packet or route.

A collection of route map statements with the same route map name is considered one route map. Within a route map, each route map statement is numbered and editable.

The statements in a route map correspond to the lines in an access list. Specifying the match conditions in a route map is similar to specifying the source and destination addresses and masks in an access list.

A major difference between route maps and access lists is that route maps can modify the route by using **set** commands.

Using Basic route-map Commands

This topic describes the basic commands used to create a route map.

Cisco.com

route-map Configuration Commands

```
router(config)#  
route-map map-tag [permit | deny] [sequence-number]
```

- Defines the conditions for policy routing

```
router(config-route-map)#  
match {conditions}
```

- Defines the conditions to match

```
router(config-route-map)#  
set {actions}
```

- Defines the action to be taken on a match

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 #8

The **route-map** command is used to define the conditions for policy routing.

route-map Command	Description
map-tag	Name of the route map
permit deny	Action taken if the route map match conditions are met
sequence-number	Sequence number that indicates the position that a new route map will have in the list of route map statements already configured with the same name

A route map consists of multiple route map statements. The router processes the statements from top to bottom, like an access list. The first matching statement found for a route is applied. Use the sequence number to insert or delete specific route map statements in a specific place in the route map. The **match** route map configuration commands define the conditions to be checked. The **set** route map configuration commands define the actions to be followed if there is a match.

A single match statement can contain multiple conditions. At least one condition in the match statement must be true in order to consider that match statement a match. A route map statement can contain multiple match statements. All match statements in the route map statement must be true in order to consider the route map statement a match.

The sequence number specifies the order in which to check conditions. For example, if there are two statements in a route map named MYMAP, one with sequence 10 and the other with sequence 20, sequence 10 is checked first. If the match conditions in sequence 10 are not met, then sequence 20 is checked. As with an access list, there is an implicit deny any at the end of a route map. The consequences of this deny depend on the function of the route map.

Configuring IP NAT with Route Maps

This topic provides a detailed example to help you understand the benefits of using route maps with NAT. The example shows the configuration and IP NAT translation table with route maps.

Route Map Configuration

Cisco.com

```
ip nat pool sales_pool 192.168.2.1 192.168.2.254 prefix-length 24
ip nat pool acct_pool 192.168.3.1 192.168.3.254 prefix-length 24
!
ip nat inside source route-map what_is_sales_doing pool sales_pool
ip nat inside source route-map what_is_acct_doing pool acct_pool
!
interface ethernet 0
 ip address 10.1.1.1 255.255.0.0
 ip nat inside
!
interface serial 0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
route-map what_is_sales_doing permit 10
match ip address 2
!
route-map what_is_acct_doing permit 10
match ip address 3
access-list 2 permit 10.1.2.0 0.0.0.255
access-list 3 permit 10.1.3.0 0.0.0.255
```

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 #9

The extended translation table in the figure is the result of adding two route maps to the configuration from the first example. In this example, the **what_is_sales_doing** route map is linked to sales_pool using the **ip nat inside source route-map what_is_sales_doing pool sales_pool** command.

An IP packet with a source IP address of 10.1.2.100 arrives on interface Ethernet 0, which is an IP NAT inside interface. The **ip nat inside source route-map what_is_sales_doing pool sales_pool** command informs the router to send the packet to the **what_is_sales_doing** route map. Sequence 10 of this route map matches the source IP address of the packet, 10.1.2.100, against access list 2, which permits the packet and match. Next, the router queries the NAT pool, called sales_pool, and gets the next address to which to translate the 10.1.2.100 packet.

When you are using a route map, the router creates a fully extended translation entry in the IP NAT translation table, which includes the source and destination TCP or UDP port numbers. When you are using only an access list, the router creates only a simple translation entry, one entry per application, without the TCP or UDP ports.

The **what_is_acct_doing** route map, together with the **ip nat inside source route-map what_is_acct_doing pool acct_pool** command, causes the router to look for source IP addresses in the 10.1.3.0/24 range and change them to source IP addresses in the 192.168.3.0/24 range.

Verifying NAT

Cisco.com

Basic IP Address Translation

Pro Inside global	Inside local	Outside local	Outside global
---	10.1.2.100	---	---
---	10.1.3.67	---	---

IP Address Translation with Route Maps

Pro Inside global	Inside local	Outside local	Outside global
udp 192.168.2.1:1024	10.1.2.100:1024	172.16.1.20:69	172.16.1.20:69
tcp 192.168.2.1:4097	10.1.2.100:4097	172.16.1.20:21	172.16.1.20:21
tcp 192.168.2.1:1084	10.1.2.100:1084	172.16.1.20:20	172.16.1.20:20
tcp 192.168.3.1:1024	10.1.3.67:1024	172.16.1.20:23	172.16.1.20:23
tcp 192.168.3.1:5553	10.1.3.67:5553	172.16.1.20:80	172.16.1.20:80

Unique TCP port numbers are used to distinguish between hosts.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 #10

DIA0_002

To examine the IP NAT translation table, use the **show ip nat translation** command.

When NAT uses only access lists, the top output is displayed. Using route maps with access lists for NAT places extended translation entries in the table.

Notice that each session now has individual entries. You can determine the IP address of each user and the applications in use.

The local device with IP address 10.1.2.100 has three sessions with an outside device with the IP address of 172.16.1.20. The full table shows that 10.1.2.100 has a TFTP session (UDP port 69) and an FTP session (TCP ports 20 and 21) with 172.16.1.20.

Local device 10.1.3.67 has two sessions with the same remote device (172.16.1.20). Its two sessions are Telnet (TCP port 23) and HTTP (TCP port 80).

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- NAT is configured on specified interfaces with the addresses to be translated defined in an ACL
- Identify the range of addresses used for translation with the *ip nat pool* command
- Route maps are complex ACLs that use *match* commands to test conditions of a packet or route
- Unlike ACLs, with route maps you can make modifications using *set* commands
- Use the *ip nat inside source route-map* command to define actions for translating IP addresses

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 #11

Next Steps

For the associated lab exercise, refer to the following sections of the course Lab Guide:

- Lab Exercise 1-1: Basic Connectivity
- Lab Exercise 1-2: NAT Using Access Lists and Route Maps

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 term refers to how devices inside the corporate network interpret the IP addresses of devices on the Internet?
- A) inside local IP address
 - B) inside global IP address
 - C) outside global IP address
 - D) outside local IP address
- Q2) How would you configure IP NAT for multiple address pools with access lists?
- A) by linking an access list to the **ip nat pool** command
 - B) by linking an access list to the **ip nat inside** command
 - C) by linking an access list to the **ip nat inside source** command
 - D) by linking an access list to the **ip nat outside** command
- Q3) What is the result in the IP network translation table when you use route maps with NAT?
- A) It simplifies the IP NAT translation table.
 - B) It tracks users by both source and destination address and TCP or UDP port numbers.
 - C) It filters out unwanted traffic.
 - D) It reduces latency through the NAT process.
- Q4) Which condition is true about default settings of route maps?
- A) At the end of a route map is an explicit permit all, and the route map does not need configuration.
 - B) At the end of a route map is an explicit deny all, and the route map does not need configuration
 - C) At the end of a route map is an implicit permit all, and the route map does not need configuration.
 - D) At the end of a route map is an implicit deny all, and the route map does not need configuration.
- Q5) Which command links a route map to an address pool?
- A) **ip nat inside source route-map test_route_map pool test_pool**
 - B) **ip nat inside source list test_route_map pool test_pool**
 - C) **ip nat inside source route-map test_route_map list 1 pool test_pool**
 - D) **ip nat inside source list 1 route-map test_route_map pool test_pool**

Quiz Answer Key

Q1) B

Relates to: Configuring IP NAT with Access Lists

Q2) C

Relates to: Configuring IP NAT with Access Lists

Q3) B

Relates to: Defining the Route Map Tool for NAT

Q4) D

Relates to: Using Basic route-map Commands

Q5) A

Relates to: Configuring IP NAT with Route Maps

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:

- Quiz 1-1: Purpose of Address Planning
- Quiz 1-2: Hierarchical Addressing Using Variable-Length Subnet Masks
- Quiz 1-3: Route Summarization and Classless Interdomain Routing
- Quiz 1-4: Understanding IP version 6

Quiz 1-1: Purpose of Address Planning

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

Objectives

This assessment tests your knowledge of how to:

- Explain the access, distribution, and core layer elements of network design in a scalable network
- List the advantages of effective network design principles
- Describe scalability, predictability, flexibility, and the ability to perform summarization as criteria of effective IP address planning

Quiz

Answer these questions:

- Q1) Which statement describes the core layer?
 - A) Consolidation occurs at this layer.
 - B) This layer is not used in a hierarchical design.
 - C) Users are generally found at this layer.
 - D) Redundancy for circuits and equipment is most common at this layer.
- Q2) Which statement describes the access layer?
 - A) Consolidation occurs at this layer.
 - B) This layer is not used in a hierarchical design.
 - C) Users are generally found at this layer.
 - D) Redundancy for circuits and equipment is most common at this layer.
- Q3) Which statement describes the distribution layer?
 - A) Consolidation occurs as this layer.
 - B) This layer is not used in a hierarchical design.
 - C) Users are generally found at this layer.
 - D) Redundancy for circuits and equipment is most common at this layer.
- Q4) Which three benefits are NOT goals of a scalable network design? (Choose three.)
 - A) scalability
 - B) cost reduction
 - C) predictability
 - D) flexibility

Quiz 1-2: Hierarchical Addressing Using Variable-Length Subnet Masks

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

Objectives

This assessment tests your knowledge of how to:

- Define the purpose of variable-length subnet masking
- Explain how to use variable-length subnet masking to maximize the use of the limited amount of IP addresses
- Explain the steps involved in variable-length subnet masking calculation

Written Exercise: Calculating VLSM

Cisco.com

Using VLSM, define appropriate subnets for addressing the networks using 192.168.49.0 /24.

Addresses for WAN Links

A Serial	_____
B Serial	_____
C Serial	_____
D Serial	_____
E Serial	_____

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-2

Quiz

You are in charge of the network shown in the figure. It consists of five LANs with 25 users on each segment and five serial links.

Allocate addressing for all links using the IP address 192.168.49.0/24.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 1-3: Route Summarization and Classless Interdomain Routing

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

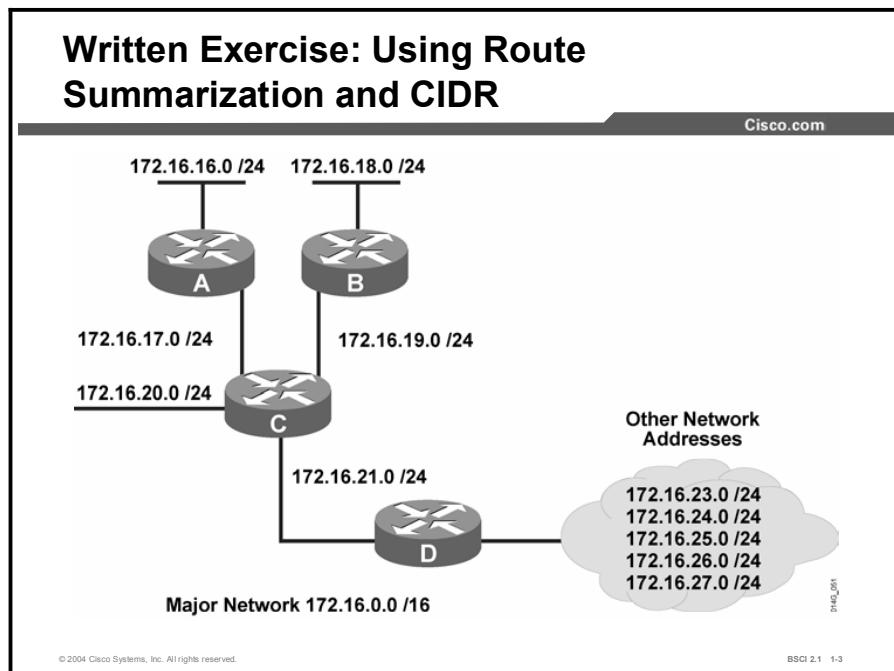
Objectives

This assessment tests your knowledge of how to:

- Describe route summarization implementation
- Calculate route summarization
- Explain classless interdomain routing implementation

Task 1

Using the following diagram, complete the table to indicate the appropriate route summarizations for the networks listed.



Router D Route Table Entries	Summarized Routes That Can Be Advertised to the Cloud from Router D

Task 2

Using the diagram from the first task, determine the most efficient and correct CIDR blocks if the first octet is 192 instead of 172.

Scoring

You have successfully completed the quiz for this lesson when you complete the exercise with correct entries..

Quiz 1-4: Understanding IP version 6

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

Objectives

This assessment tests your knowledge of how to:

- Recall the purpose and benefits of IPv6
- Describe IPv6 addressing
- List the fields in the header of an IPv6 address
- Explain how a 6to4 tunnel works

Quiz

Answer these questions:

- Q1) Which feature is NOT important in IPv6?
- A) larger address space
 - B) security
 - C) shorter header
 - D) simpler header
 - E) autoconfiguration
- Q2) How many bytes is an IPv6 address?
- A) 4
 - B) 8
 - C) 12
 - D) 16
- Q3) In the IPv6 address format a colon (:) is used to separate _____.
A) each byte in the address
B) every 2 bytes
C) every 4 bytes
D) none of the above
- Q4) Which IPv6 address is equivalent to ff01 ::1?
- A) ff01 :0 :0 :1
 - B) ff01 :1 :1 :1
 - C) ff01 :0 :0 :0 :0 :0 :1
 - D) ff01 :1 :1 :1 :1 :1 :1
- Q5) In IPv6 autoconfiguration, what does “RA” mean?
A) remote access
B) reusable address
C) remote address
D) router advertisement

- Q6) What type of information is sent when performing RA autoconfiguration?
- A) network prefix and default gateway
 - B) complete IPv6 address for the new host
 - C) complete IPv6 address of router
 - D) link-layer address of router
- Q7) During autoconfiguration, a final host IPv6 address will consist of the learned network prefix combined with the link layer of the host address.
- A) true
 - B) false
- Q8) In the IPv6 header, the traffic class field is similar to which field in the IPv4 header?
- A) fragmentation field
 - B) fast-switching field
 - C) ToS field
 - D) CEF field
- Q9) What function does the flow label field in the IPv6 header perform?
- A) priority queuing
 - B) custom queuing
 - C) multilayer switching techniques
 - D) fragmentation
- Q10) How is the TTL field in the IPv4 header represented in IPv6?
- A) TTL has not changed from IPv4.
 - B) It is the hop limit.
 - C) TTL is not required in IPv6.
 - D) It is the maximum routers field.
- Q11) List three uses for extension headers in IPv6.
- A) _____
 - B) _____
 - C) _____
- Q12) IPv6 uses IPSec for security; it is built into the specification.
- A) true
 - B) false
- Q13) Which statement best describes dual stack?
- A) IPv6 running twice as fast as IPv4
 - B) IPv6 packets encapsulated into an IPv4 header
 - C) IPv6 and IPv4 running simultaneously on each router interface
- Q14) Which statement describes an overlay tunnel?
- A) IPv6 running twice as fast as IPv4
 - B) IPv6 packets encapsulated into an IPv4 header
 - C) IPv6 and IPv4 running simultaneously on each router interface

- Q15) Which is an attractive feature of a 6to4 tunnel?
- A) The tunnel automatically establishes itself.
 - B) The tunnel requires manual configuration.
 - C) The routers require no special code to support this tunnel technique.
 - D) Tunnel routers are not required at both ends of the tunnel.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 1-1: Purpose of Address Planning

- Q1) D
- Q2) C
- Q3) A
- Q4) A, C, D

Quiz 1-2: Hierarchical Addressing Using Variable-Length Subnet Masks

Written Exercise: Calculating VLSM

Cisco.com

Using VLSM, define appropriate subnets for addressing the networks using 192.168.49.0 /24.

Subnets and Hosts:

- 192.168.49.0/27 25 Users (Subnet A)
- 192.168.49.32/27 25 Users (Subnet B)
- 192.168.49.64/27 25 Users (Subnet C)
- 192.168.49.96/27 25 Users (Subnet D)
- 192.168.49.128/27 25 Users (Subnet E)

WAN Addresses:

A Serial	— 192.168.49.224/27
B Serial	— 192.168.49.228/27
C Serial	— 192.168.49.232/27
D Serial	— 192.168.49.236/27
E Serial	— 192.168.49.240/27

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 1-4

Subnet	,	Valid Hosts	,	Broadcast
192.168.49.224	,	192.168.49.225 to 192.168.49.226	,	192.168.49.227
192.168.49.228	,	192.168.49.229 to 192.168.49.230	,	192.168.49.231
192.168.49.232	,	192.168.49.233 to 192.168.49.234	,	192.168.49.235
192.168.49.236	,	192.168.49.237 to 192.168.49.238	,	192.168.49.239
192.168.49.240	,	192.168.49.241 to 192.168.49.242	,	192.168.49.243

Quiz 1-3: Route Summarization and Classless Interdomain Routing

Task 1

Router D Route Table Entries	Summarized Routes That Can Be Advertised to the Cloud from Router D
172.16.16.0 /24	172.16.16.0 /22
172.16.17.0 /24	172.16.20.0 /23
172.16.18.0 /24	
172.16.19.0 /24	
172.16.20.0 /24	
172.16.21.0 /24	

Task 2

All addresses are 192.16.xx.0/24 as with the 172 address space.

What router D can show is 192.16.16.0/22, which encompasses subnets 192.16.16.0 through 192.16.19.255 and subnet 192.16.20.0/23, which has 192.16.20.0 through 192.16.21.255.

Quiz 1-4: Understanding IP Version 6

- Q1) C
- Q2) D
- Q3) B
- Q4) C
- Q5) D
- Q6) A
- Q7) A
- Q8) C
- Q9) C
- Q10) B
- Q11) Answers could be any of the following:

- Hop-by-hop options header
- Destination options header (when the routing header is used)
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination options header
- Upper-layer header

- Q12) A
- Q13) C
- Q14) B
- Q15) A

Module 2

Routing Principles

Overview

This module examines advanced IP routing principles, including static and dynamic routing characteristics, classful and classless routing, and automatic route summarization across network boundaries. It explains the difference between distance vector, link-state, and hybrid routing protocols. Also included is a comparison of IP routing protocols.

Module Objectives

Upon completing this module, you will be able to implement advanced IP routing principles and protocols to determine the appropriate IP routing protocol for your network.

Module Objectives

Cisco.com

- **Select and implement the most effective method of IP routing for the topology of your network and its requirements**
- **Compare and contrast the concepts and operation of classful and classless IP routing protocols**
- **Determine the appropriate IP routing protocol for your network**

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- **IP Routing Overview**
- **Characteristics of Routing Protocols**
- **IP Routing Protocol Comparison**
- **Lesson Assessments**

IP Routing Overview

Overview

Routers forward packets toward destination networks. To forward the packets, routers must understand these remote networks and determine the best way to reach them. This lesson addresses the ways that routers learn about networks. This lesson also identifies the concepts of IP routing using static and dynamic routes.

Relevance

Network administrators are responsible for choosing whether to implement static or dynamic routing. To make a responsible choice, network administrators must understand the difference between static and dynamic routing.

Objectives

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

- Explain the principles of static routing
- Configure static routing
- Describe the principles of dynamic routing
- Discuss the principles of ODR
- Configure ODR

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Principles of Static Routing**
- **Configuring a Static Default Route**
- **Principles of Dynamic Routing**
- **Principles of On-Demand Routing**
- **Configuring ODR**
- **Summary**
- **Quiz**

Principles of Static Routing

It is important to understand when to use and when not to use a static route. This topic examines how to use static routing appropriately and demonstrates the necessary commands to configure static routes.

Principles of Static Routing

Cisco.com

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

- **Creates a static route**

```
core1# config t
core1(config)#ip route 10.2.0.0 255.255.0.0 10.1.1.1
```
- **Resulting static route entry in the routing table**

```
core1# show ip route
<output omitted>
S  10.2.0.0/16 [1/0] via 10.1.1.1
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-4

Routers must recognize destination networks so they can forward packets to them. A router knows about the networks directly attached to its interfaces but must rely on outside information for remote networks. There are two ways that a router can recognize remote networks: An administrator can manually configure the information (static routing), or a router can learn from other routers (dynamic routing). A routing table can contain both statically and dynamically recognized routes.

Network administrators must choose between using static routing, dynamic routing, or a combination of both. A static route can be used in the following circumstances:

- When it is undesirable to have the routing table update traffic that is created by dynamic routing protocols forwarded across low-bandwidth links, such as a dialup link.
- When the administrator needs total control over the routes used by the router.
- When a backup to a dynamically recognized route is necessary.
- When it is necessary to reach a network accessible by only one path (a stub network). For example, in the example figure, there is only one way for router A to reach the 10.2.0.0/16 network on router B. You can configure a static route on router A to reach the 10.2.0.0/16 network via 10.1.1.
- When a router is underpowered and does not have the CPU or memory resources necessary to handle a dynamic routing protocol.
- When a route should appear to the router as a directly connected network.

A perfect match for static routing is a hub-and-spoke design, with all remote sites defaulting to the central site and the one or two routers at the central site having a static route for all subnets at each remote site. However, without proper design, as the network grows into hundreds of routers with each router having numerous subnets, the number of static routes on each router also increases. Each time a new subnet or router is added, an administrator must add a static route to the new networks on a number of routers. The administrative burden to maintain this network could become excessive, making dynamic routing a better choice.

Another drawback to static routing is that when a topology change occurs on the internetwork, an administrator may have to reroute traffic by configuring new static routes around the problem area. With dynamic routing, the routing process automatically discovers whether any alternate routes exist and reroutes without administrator intervention.

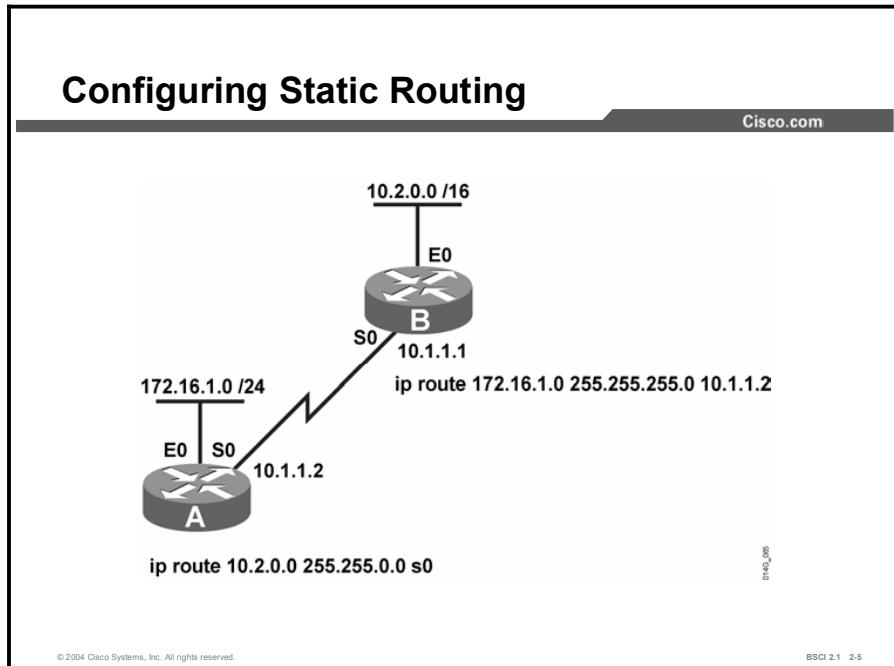
The **ip route** command creates a static route. The **show ip route** command verifies the resulting static entry in the IP routing table. A static route must be configured on the routers on both sides of the link. Otherwise, because there are no routing protocols going across that link, the remote router would not be able to return the packet. There would be only one-way communication.

Specify either a next-hop IP address or an exit interface to notify the router of the direction to send traffic. If the next-hop IP address is used, it should be the IP address of the router on the other end of the link. If the exit interface is used, the local router will send data to the router on the other end of its attached link. When an exit interface is specified, the router considers this a directly connected route.

ip route Command	Description
address	IP address of the next hop that can be used to reach the destination network
distance	(Optional) Administrative distance to be assigned to this route
interface	The local router outbound interface to be used to reach the destination network
permanent	Specifies that the route will not be removed from the routing table even if the interface associated with the route goes down
prefix mask	IP network and subnet mask for the remote network to be entered into the IP routing table
tag	(Optional) Value that can be used as a match value in route maps

Note	Use static routes pointing to an interface on point-to-point interfaces only, because on multiaccess interfaces the router will not know the specific address to which to send the information. On point-to-point interfaces, the information is sent to the only other device on the network.
-------------	--

Example

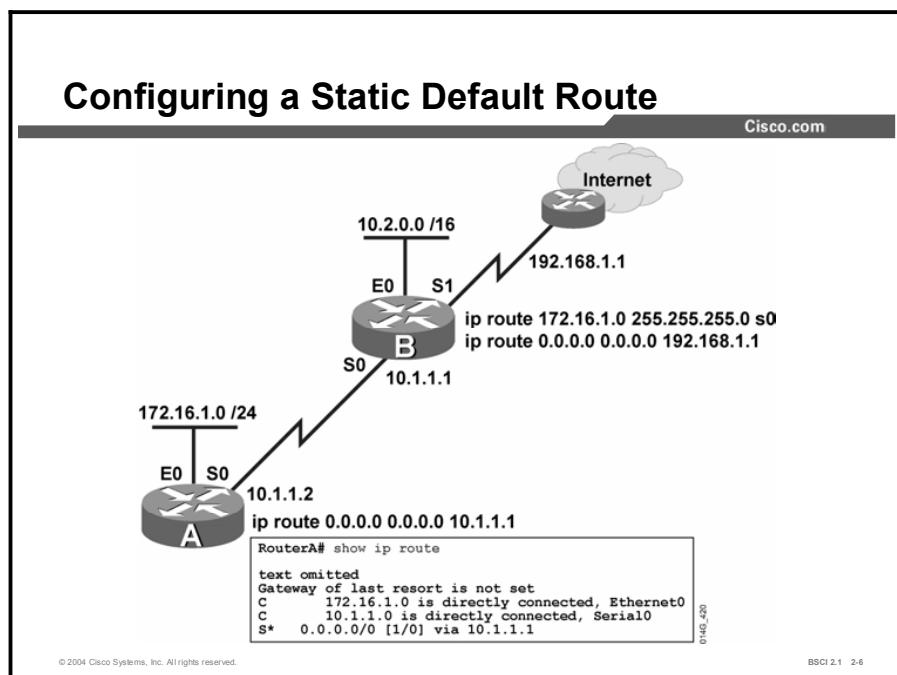


In the figure shown, router A is a stub router: it has no other routers beyond it. If router B sends data to any device in the 172.16.1.0/24 network, it must be sent through router A. Similarly, if router A needs to send data to any device in the 10.2.0.0/16 network, it must go through router B. The figure shows the static routes created on both router A and router B to accomplish this connection.

Router A recognizes the directly connected networks 172.16.1.0 and 10.1.1.0. It needs a route to the remote network 10.2.0.0. Router B knows about the directly connected networks 10.2.0.0 and 10.1.1.0; it needs a route to the remote network 172.16.1.0. Notice that on router B, the next-hop IP address of the router A serial interface has been used. On router A, however, the **ip route** command specifies the exit interface.

Configuring a Static Default Route

This topic explains when to use a static default route and describes its configuration.



In some circumstances, a router does not need to recognize remote networks at all. The router is configured to send all traffic, or all traffic for which there is no entry in the routing table, in a particular direction known as a default route. Default routes are either dynamically advertised using routing protocols or are statically configured.

To create a static default route, use the normal **ip route** command. However, the destination network and its subnet mask are both 0.0.0.0. This address is a type of wildcard designation; any destination network will match. Because the router tries to match the longest common bit pattern, a network listed in the routing table is used before the default route. If the destination network is not listed in the routing table, then the default route is used.

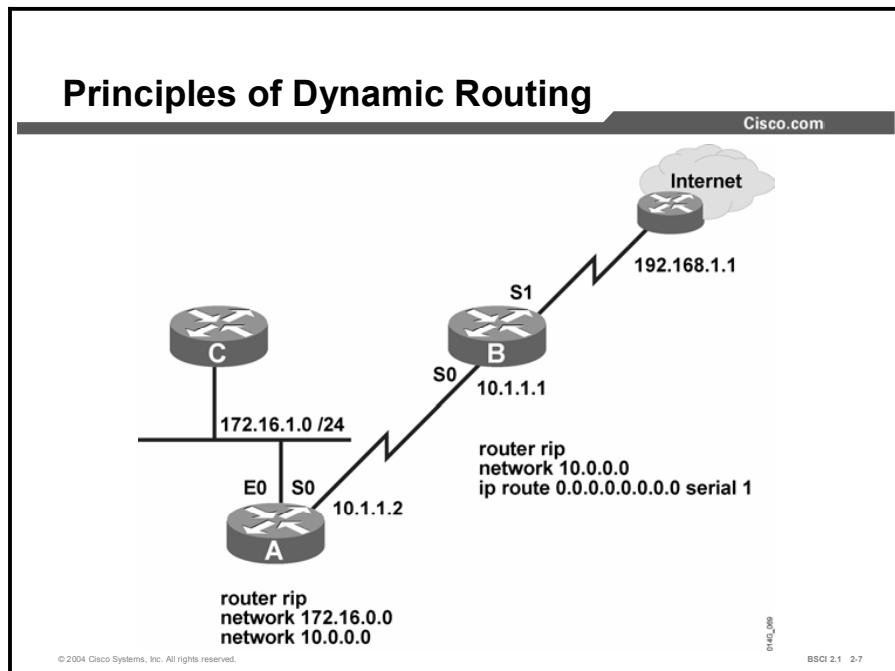
Example

In the figure, on router A, the static route to the 10.2.0.0 network has been replaced with a static default route pointing to router B. On router B, a static default route has been added pointing to its Internet service provider (ISP). Traffic from a device on the router A 172.16.1.0 network bound for a network on the Internet is sent to router B. Router B recognizes that the destination network does not match any specific entries in its routing table and sends that traffic to the ISP. It is then the responsibility of the ISP to route that traffic to its destination.

To reach the 172.16.1.0/24 network, router B still needs a static route pointing out its serial 0 interface.

Principles of Dynamic Routing

Dynamic routing allows the network to adjust to changes in the topology automatically, without administrator involvement. This topic describes standard dynamic routing principles. The network statement is a necessary part of configuring most IP routing protocols, but its function is often misunderstood. This topic also examines the effect of the network statement on various protocols.



A static route cannot respond dynamically to changes in the network. If a link fails, the static route is no longer valid if it goes through that failed link. A new static route must be configured. If a new router or new link is added, that information must also be configured on every router in the network. In a very large or unstable network, these changes can lead to considerable work for network administrators. It can also take a long time for every router in the network to receive the correct information. In situations like these, it may be better to have the routers receive information about networks and links from each other using a dynamic routing protocol.

When using a dynamic routing protocol, the administrator configures the routing protocol on each router. The routers then exchange information about the reachable networks and the state of each network. Routers exchange information only with other routers running the same routing protocol. When the network topology changes, the new information is dynamically propagated throughout the network, and each router updates its routing table to reflect the changes. Some examples of dynamic routing protocols are as follows:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS) Protocol
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

The distance to the network, which is called the metric or cost, is included in the information exchanged by routers. Different routing protocols base their metric on different measurements: hop count, interface speed, or more complex metrics. Most routing protocols maintain databases containing all the networks that each routing protocol recognizes and all the paths to each network. If a router recognizes more than one way to reach a network, it will compare the metric for each different path and choose the path with the lowest metric. If there are multiple paths with the same metric, a maximum of six can be installed in the routing table, and the router can perform load balancing between them. Interior Gateway Routing Protocol (IGRP) and EIGRP can also perform load balancing between unequal-cost paths.

To configure an IP dynamic routing protocol, use the **router protocol** command. Protocols other than RIP also require specification of either an autonomous system or a process number. For every protocol except IS-IS and BGP, you will also need the **network** command under the router configuration mode.

For RIP, IGRP, EIGRP, and OSPF, the **network** command tells the router which interfaces are participating in that routing protocol. Any interface that has an IP address that falls within the range specified in the network statement is considered active for that protocol. In other words, the router sends updates from the specified interfaces and expects to receive updates from the same interfaces. Some protocols will look for neighbors by sending hello packets out those interfaces. Thus, because a network statement identifies interfaces on the local router, it is configured only for directly connected networks. A router also originates advertisements for the networks connected to the specified interfaces.

RIP and IGRP use only major classful networks to determine the interfaces participating in the protocol. EIGRP and OSPF permit exact specification of interfaces with a combination of a subnet or interface address and a wildcard mask.

The network statement functions differently in BGP. BGP requires its neighbors to be statically configured. The network statement in BGP notifies the router to originate an advertisement for that network. Without a network statement, BGP passes along advertisements it receives from other routers, but does not originate any network advertisements itself. In BGP, the network listed in the network statement does not have to be a directly connected network because it is not identifying interfaces on the router as it would in other protocols.

Integrated IS-IS does not use the network statement. Instead, interfaces participating in the IS-IS routing process are identified under the interface configuration mode.

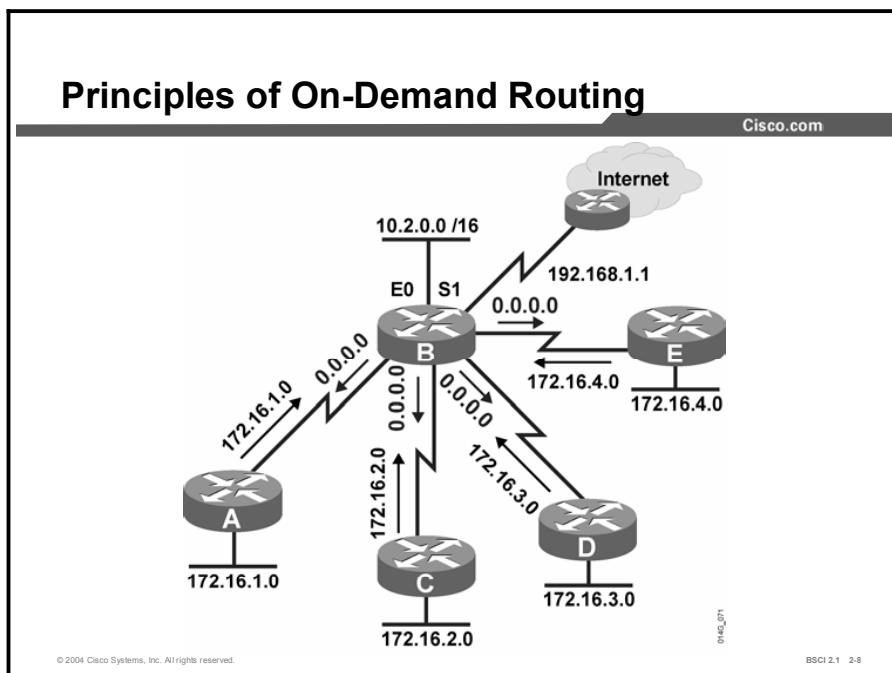
Example

As an example, the previous figure showed the commands necessary to configure RIP to run on routers A and B. Router A has two directly attached networks and needs RIP to search for neighbors on both of those interfaces. Therefore, network statements are configured for both the 172.16.1.0 network and the 10.1.1.0 network. Router A sends RIP packets out interfaces E0 and S0. The neighbors also receive an advertisement for the networks that are attached to those interfaces.

Router B also has two directly attached networks. However, router B wants only the network it shares with router A to participate in RIP. Therefore, a network statement is configured only for the 10.1.1.0 network. Router B has a static default route pointing toward its ISP to reach other networks. Router B sends RIP packets out its interface serial 0, but not out interface serial 1. It does not advertise the 192.168.1.0 network attached to serial 1 or the static default route unless specifically configured to do so.

Principles of On-Demand Routing

This topic describes On-Demand Routing (ODR), which is a Cisco proprietary alternative to static routes.



A drawback to static routes is that they must be manually configured and updated when the network topology changes. A drawback to dynamic routing protocols is that they use network bandwidth and router resources. In a hub-and-spoke network with hundreds of spokes, both the configuration needed for static routes and the resource usage of dynamic routing could be considerable.

There is a third option—ODR. ODR uses the Cisco Discovery Protocol (CDP) to carry network information between spoke (stub) routers and the hub. ODR provides IP routing information with minimal overhead compared to a dynamic routing protocol. ODR requires less manual configuration than static routes.

ODR is applicable in a hub-and-spoke topology only. In this type of topology, each spoke router is adjacent only to the hub. Another term for this topology is “stub router.” The stub router may have some LAN networks connected to it and typically has a WAN connection to the hub router. The hub router needs to recognize the networks connected to each spoke but the spokes need only a default route pointing to the hub.

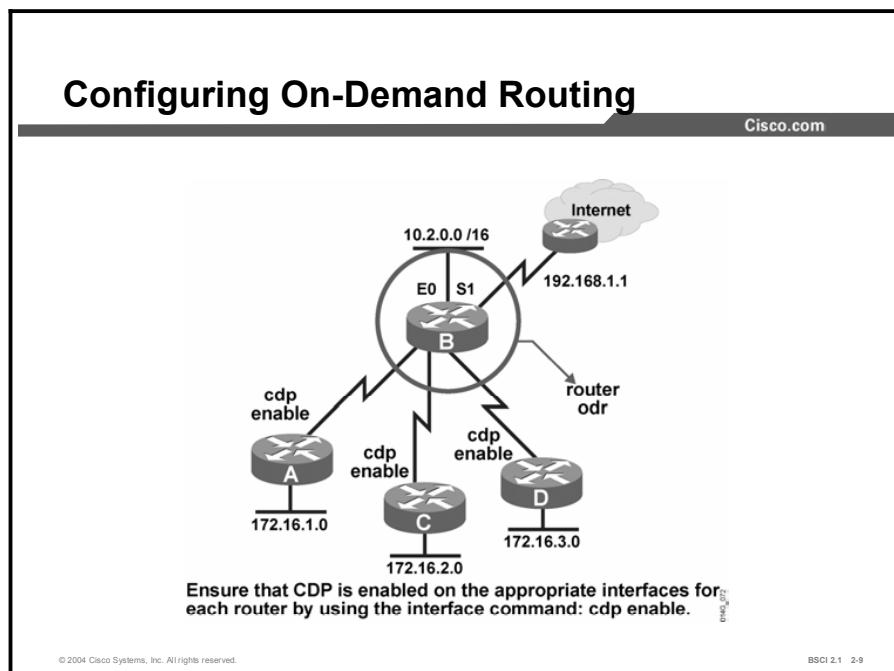
When ODR is configured, the stub routers use CDP to send IP prefix information to the hub router. Stub routers send prefix information for all their directly connected networks. ODR reports the subnet mask, so it supports variable-length subnet masking (VLSM).

The hub router, in turn, sends a default route to the spokes that point back to itself. It installs the stub networks reported by ODR in its routing table, and the hub router can be configured to redistribute them into a dynamic routing protocol. For a next-hop address, the hub router uses the IP address of the spoke routers as reported to it by CDP.

ODR is not a true routing protocol because the information exchanged is limited to IP prefixes and a default route. There is no metric information reported by ODR; the hub router uses a hop count of one as the metric for all routes reported via ODR. However, by using ODR, routing information for stub networks can be obtained dynamically without the overhead of a dynamic routing protocol, and default routes can be provided to the stub routers without manual configuration.

Configuring ODR

ODR is an attractive alternative to static routing because of the simple configuration required. This topic describes how to configure ODR.



The configuration of ODR is done on the hub router using the global **router odr** command.

On the stub router, no IP routing protocol must be configured. In fact, from the standpoint of ODR, a router is automatically considered a stub when no IP routing protocols have been configured.

You may want to tune ODR with some of the optional commands. A distribute list can be placed in the router configuration mode to control the network information that is recognized through ODR. The ODR timers can be adjusted with the **timers basic** command in router configuration mode.

Because the spoke routers receive only a default route from the hub router, all network information beyond their own stub networks is hidden from them. If information about the stub networks needs to be propagated to other parts of the enterprise, it can be redistributed into dynamic routing protocols by the hub router with an appropriate metric.

ODR relies on the CDP to carry the information between the hub router and the spoke routers. Therefore, CDP must be enabled on the links between the hub router and spokes. Cisco routers by default have CDP enabled both globally and per interface. However, on some WAN links, such as ATM, CDP must be explicitly enabled.

The CDP updates are sent as multicasts. On WAN links that require mappings, such as dialer links and Frame Relay, it is important to use the **broadcast** keyword in the mapping statements. Allowing broadcasts also allows multicasts across the link. CDP uses Subnetwork Access Protocol (SNAP) frames, so it will run on all media that support SNAP.

CDP updates are sent every 60 seconds by default. This setting may be too infrequent in rapidly changing networks or too frequent in stable ones. The timers can be adjusted by the **cdp timer** global command.

CDP settings can be verified by using the **show cdp interface** command.

Example

Configuring On-Demand Routing (Cont.)

Cisco.com

Routing table with ODR routes:

```
Router B#show ip route
<output omitted>
172.16.0.0/16 is subnetted, 4 subnets
o 172.16.1.0/24 [160/1] via 10.1.1.2, 00:00:23, Serial0
o 172.16.2.0/24 [160/1] via 10.2.2.2, 00:00:03, Serial1
o 172.16.3.0/24 [160/1] via 10.3.3.2, 00:00:16, Serial2
o 172.16.4.0/24 [160/1] via 10.4.4.2, 00:00:45, Serial3
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-10

Once ODR is configured and running, routes from the stub routers are identified in the routing table at the hub router with an *o* character. Notice in the example that the metric is 1 and the administrative distance for ODR is 160.

The routing table for each of the spoke routers contains only its connected networks and a static default route injected by ODR from the hub router.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configure static routes to keep manual control of routing change updates and to eliminate routing update overhead.**
- **Static routes are used for stub networks and backup routes for dynamic routing protocols.**
- **Configure static routes and static default routes using the Cisco IOS command ip route.**
- **Configure dynamic routing to allow the routing protocol to automatically adjust for topology changes and perform routing communication for table entry updates.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-11

Summary (Cont.)

Cisco.com

- **Use the router protocol command to select the dynamic routing protocol; use the network command with RIP, IGRP, EIGRP, and OSPF.**
- **For hub-and-spoke topologies, Cisco-proprietary ODR is an alternative to static routes or dynamic routing.**
- **ODR uses CDP to provide automatic routing updates with minimal overhead.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-12

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 statements about static routing are true? (Choose two.)
- A) A static route must be manually configured.
 - B) A router will dynamically update static routing information.
 - C) Static and dynamic routes cannot be used on the same router.
 - D) When used appropriately, static routes can help a network perform more efficiently.
- Q2) Which two statements are true? (Choose two.)
- A) A static route needs to be configured on one end of the link only; the router on the other end will autodetect the route by default.
 - B) When the *distance* option is used with the **ip route** command, the router assigns that figure as the metric for the route.
 - C) Static routes are one-way only and must be configured on both ends of a link.
 - D) In the **ip route** command, either the next-hop IP address or the exit interface can be specified.
- Q3) Which three components are parameters of the **ip route** command? (Choose three.)
- A) the local network address and subnet mask
 - B) the remote network address and subnet mask
 - C) both the local router exit interface and the next-hop IP address
 - D) either the local router exit interface or the next-hop IP address
 - E) an optional administrative distance value
- Q4) In which two instances is it appropriate to use a default route? (Choose two.)
- A) All traffic to remote networks must go to the same next-hop router.
 - B) There are many exit points from the network.
 - C) The router does not need to know about all the remote networks.
 - D) The router needs to be able to recognize all the remote networks.
- Q5) Which two are metrics of a dynamic routing protocol? (Choose two.)
- A) always tells the number of hops between the network and the local router
 - B) is a measurement of the monthly charge for the line
 - C) varies by protocol
 - D) is the distance to the network from the local router

- Q6) What is the maximum number of equal-cost paths that a router can install in its IP routing table?
- A) one
 - B) three
 - C) four
 - D) six
- Q7) Which two statements identify the purpose of the network statement in EIGRP? (Choose two.)
- A) tells the router to originate advertisements for that network
 - B) specifies the local interfaces participating in EIGRP
 - C) specifies the remote networks that should be advertised
 - D) tells the router to search for neighbors outside of that interface
- Q8) What are two functions of the network statement in BGP? (Choose two.)
- A) it tells the router to originate advertisements for that network
 - B) it specifies the local interfaces participating in EIGRP
 - C) it specifies the remote networks that should be advertised
 - D) it tells the router to search for neighbors outside of that interface
- Q9) Which two statements about ODR are true? (Choose two.)
- A) ODR is used in a hub-and-spoke topology.
 - B) ODR is a classful routing protocol.
 - C) Spoke routers send a default route to the hub router, and the hub router sends network information to the spokes.
 - D) Spoke routers send information about their networks to the hub router, and the hub router sends a default route to the spokes.
- Q10) Which protocol does ODR use to carry its network information?
- A) RIP
 - B) X.25
 - C) VTP
 - D) CDP
- Q11) Which configuration task must you perform on the spoke routers when you are using ODR?
- A) You must start ODR by using the **router odr** command.
 - B) You must tag the networks to be advertised as ODR routes.
 - C) No configuration is necessary on the stub router.

Quiz Answer Key

Q1) A, D

Relates to: Principles of Static Routing

Q2) C, D

Relates to: Principles of Static Routing

Q3) B, D, E

Relates to: Principles of Static Routing

Q4) A, C

Relates to: Configuring a Static Default Route

Q5) C, D

Relates to: Principles of Dynamic Routing

Q6) D

Relates to: Principles of Dynamic Routing

Q7) B, D

Relates to: Principles of Dynamic Routing

Q8) A, C

Relates to: Principles of Dynamic Routing

Q9) A, D

Relates to: Principles of On-Demand Routing

Q10) D

Relates to: Configuring On-Demand Routing

Q11) C

Relates to: Configuring On-Demand Routing

Characteristics of Routing Protocols

Overview

Routing protocols share many features with each other, but they can be classified into different categories, such as link state, distance vector, or a hybrid of these two. IP routing protocols can also be classified as either classful or classless. This lesson examines the characteristics and operations of classful and classless routing protocols.

Relevance

Most modern networks use one of the classless routing protocols. With an understanding of classless behavior, administrators are able to make the most efficient use of these protocols. Classful routing protocols are older protocols; however, you must understand them in the context of current networking requirements. Some classless routing protocols behave classfully by default. Therefore, it is important to understand classful behavior, such as automatic network boundary summarization and classful protocol interpretation of the routing table.

Objectives

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

- Describe the concepts of classful routing protocols
- Describe automatic network boundary route summarization in a classful routing protocol
- Interpret a classful routing table
- Identify concepts of classless routing protocols
- Discuss network boundary route summarization in a classless routing protocol
- Contrast the effects of the **auto-summary** and **no auto-summary** commands
- Describe the RIPv1 method of distance-vector routing
- Identify the characteristics and configurations of RIPv2

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Classful Routing Protocol Concepts**
- **Automatic Network Boundary Summarization in a Classful Routing Protocol**
- **Examining a Classful Routing Table**
- **Classless Routing Protocol Concepts**
- **Automatic Network Boundary Summarization Using RIPv2 and EIGRP**
- **The auto-summary Command for RIPv2 and EIGRP**
- **Characteristics of RIPv1**
- **Characteristics and Configuration of RIPv2**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 2-3

Classful Routing Protocol Concepts

This topic reviews the concepts that determine how classful routing protocols work.

Concepts of Classful Routing

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.**
- **Network boundary summarization is done automatically.**
- **Example of classful routing protocols:**
 - Routing Information Protocol version 1 (RIPv1)
 - Interior Gateway Routing Protocol (IGRP)

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-4

When classful protocols were originally developed, networks were very different from those used now. The best modem speed was 300 bps, the largest WAN line was 56 kbps, router memory was under 640 KB, and processors were running in the kHz range. Routing updates had to be small enough not to monopolize the WAN link bandwidth. In addition, routers did not have the resources to maintain up-to-date information about every subnet.

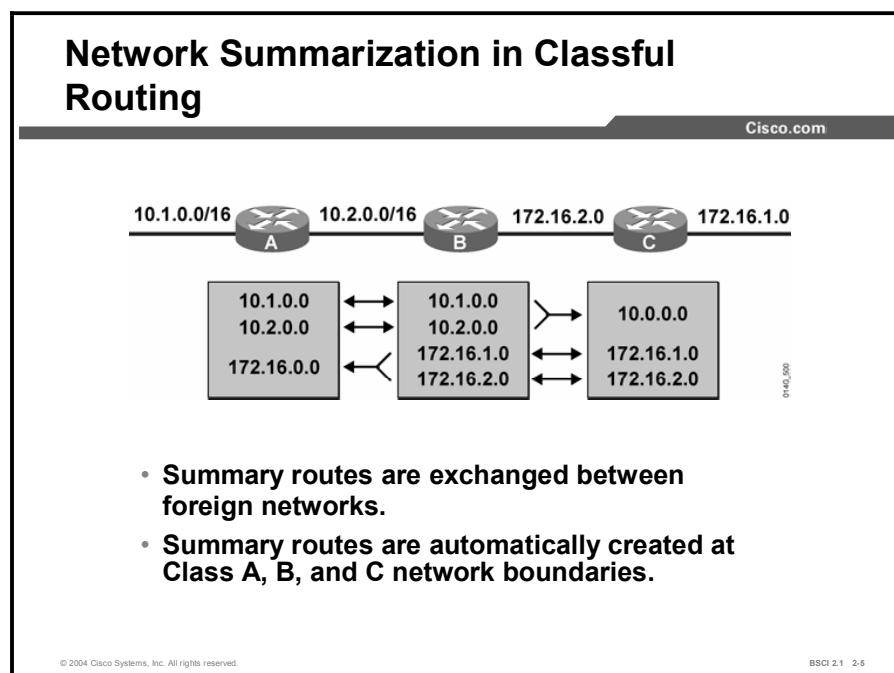
A classful routing protocol does not include subnet mask information in its routing updates. Because no subnet mask information is known, when a classful router sends or receives routing updates, the router makes assumptions about the subnet mask being used by the networks listed in the update. These assumptions are based on IP address class. 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 than the one configured on the receiving interface, the router applies the default classful mask by IP address class. The IP address classes and their default classful masks are as follows:
 - 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.

All subnets of the same major network, Classes A, B, and C, must use the same subnet mask when using a classful routing protocol. Otherwise, routers may assume incorrect subnet information. Routers running a classful routing protocol perform automatic route summarization across network boundaries.

Automatic Network Boundary Summarization in a Classful Routing Protocol

Classful routing protocols make assumptions about networks based on their IP address class. These assumptions lead to automatic summarization of routes when routers send updates across major classful network boundaries. This topic describes the summarization of routes and how updates are sent across network boundaries.



Routers send update packets from their interfaces to other connected routers. The router sends the entire subnet address when an update packet involves a subnet of the same classful network as the IP address of the transmitting interface. The router assumes that the network and the interface use the same subnet mask.

The router that receives the update also makes the same assumption. If that route was using a different subnet mask, then the router would have incorrect information in its routing table. Thus, when using a classful routing protocol, it is important to use the same subnet mask on all interfaces belonging to the same classful network.

When a router using a classful routing protocol sends an update regarding a subnet of a classful network across an interface belonging to a different classful network, the router assumes that the remote router will use the default subnet mask for that class of IP address. Therefore, when the router sends the update, it does not include the subnet information. The update packet contains only the classful network information. This process is autosummarization across the network boundary. The router sends a summary of all the subnets in that network by sending only the major network information. Classful routing protocols automatically create a classful summary route at major network boundaries. Classful routing protocols do not allow summarization at other points within the major network address space.

The router that receives the update behaves in a similar fashion. When an update contains information about a different classful network than the one in use on its interface, the router applies the default classful mask to that update. The router must determine the correct subnet mask to apply because the update does not contain subnet mask information.

Example

In the figure, router A advertises the 10.1.0.0 subnet to router B because the interface connecting them belongs to the same major classful 10.0.0.0 network. Router B uses a 16-bit subnet mask on the interface between itself and router A. When router B receives the update packet, it assumes that the 10.1.0.0 subnet uses the same 16-bit mask as the one used on its 10.2.0.0 subnet.

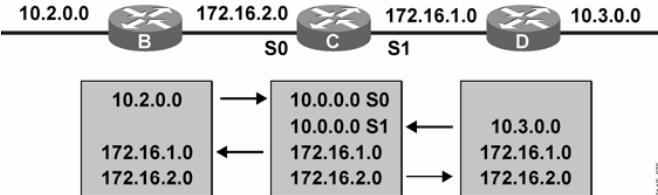
Routers B and C include the subnet information when they exchange information about the 172.16.0.0 network because the interface connecting them belongs to the same major classful 172.16.0.0 network. Therefore, the routing table of router B has information about all the subnets that are in use in the network.

However, router B summarizes 10.1.0.0 and 10.2.0.0 subnets to 10.0.0.0 before sending the routing information to router C. This summarization occurs because the update crosses a major network boundary. The update goes from a subnet of network 10.0.0.0, subnet 10.2.0.0, to a subnet of another major network, network 172.16.0.0.

Router B summarizes the 172.16.1.0 and 172.16.2.0 subnets to 172.16.0.0 before sending them to router A. Therefore, the routing table of router A contains summary information about only the 172.16.0.0 network. The routing table of router C contains summary information about only the 10.0.0.0 network.

Classful Subnet Issues

Cisco.com



9140-015

- All router interfaces within the same network must have the same subnet mask.
- This approach may not fully use available allocation of host addresses.
- All subnets of the same major network must be contiguous.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-6

Discontiguous subnets occur when a different major network separates subnets of a major network. In the figure, router D has a subnet of the 10.0.0.0 network connected to it. It is important to notice the router C routing table. It has two summary routes to the 10.0.0.0 network: one through router B and one through router D. Because these paths have equal metrics, both paths are installed in the routing table. Router C attempts to perform load balancing over both paths. Traffic does not always reach its destination. Router C has a 50-50 chance of correctly routing the packets to a subnet of network 10.0.0.0. For example, router C would not know exactly which interface (serial 0 or serial 1) to use to reach the 10.2.0.0 and 10.3.0.0 subnets.

For this reason, do not permit discontiguous subnets when using classful routing protocols. All subnets of the same major network must be contiguous. Discontiguous subnets are not visible to each other because subnets are not advertised across the network boundary. A classful routing protocol assumes that it has knowledge of all existing subnets of a major classful network.

When you are performing subnetting while using classful routing protocols, assign all subnets of the same major network to the same subnet mask. This technique is called fixed-length subnet masking (FLSM). FLSM ensures consistency for correctly advertised subnetwork routes. However, the consistency of a subnet mask has a potential disadvantage from the standpoint of efficient address allocation. For example, a 27-bit mask allocates the proper number of host addresses for an Ethernet segment needing 30 hosts; however, 30 addresses are not used on a point-to-point serial link. A point-to-point serial link requires only two addresses. Therefore, 28 addresses are wasted.

Examining a Classful Routing Table

This topic describes the features of the classful routing table.

Interpreting the IP Routing Table with a Classful Protocol

Cisco.com

```
plr3# show ip route
<output omitted>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
    10.0.0.0/24 is subnetted, 3 subnets,
    R      10.1.1.0/24 [120/1] via 10.1.2.2, 00:00:05, Ethernet0
    C      10.1.2.0/24 is directly connected, Ethernet0
    R      10.1.3.0/24 [120/2] via 10.1.2.2, 00:00:05, Ethernet0
    R      192.168.24.0/24 [120/2] via 10.1.2.2, 00:00:16, Ethernet0
    R      172.16.0.0/16 [120/3] via 10.1.2.2, 00:00:16, Ethernet0
    R*     0.0.0.0/0 [120/3] via 10.1.2.2, 00:00:05, Ethernet0
```

Where will the router send traffic bound for the following destinations?

- 192.168.24.3
- 172.16.5.1
- 10.1.2.7
- 200.100.50.0
- 10.2.2.2

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 2-7

Autosummarization can be viewed by looking at the IP routing table. This topic examines the routing table and how a classful routing protocol forwards traffic.

This figure shows an example of the output from the **show ip route** command executed on a router running Routing Information Protocol (RIP). What would the router do with traffic that is bound for various destinations? Some examples of traffic destinations are as follows:

- 192.168.24.3
- 172.16.5.1
- 10.1.2.7
- 200.100.50.0
- 10.2.2.2

The routing table contains routes to the first three destination networks in the bulleted list. There is no route to the fourth destination, 200.100.50.0, but there is a default route. The router uses the default route for the fourth destination.

The fifth destination, 10.2.2.2, is bound for an unknown subnet of a major network that is in the routing table. By default, a classful routing protocol assumes that it knows about all subnets of a network in its routing table. It discards traffic routed to any unknown subnets, so the packet to 10.2.2.2 is discarded by default.

The behavior of the classful routing protocol changes when you are using the **ip classless** command.

The IP Classless Command

Cisco.com

```
Router(config)# ip classless
```

- Replaces the default behavior of classful routing protocols to match against only known subnets of a major network
- Changes default behavior of classful routing protocol for unknown subnets
- On by default in Cisco IOS Release 12.0 and later
- Has no effect on most classless routing protocols because they use the longest-match criterion by default

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-8

The **ip classless** command causes a classful routing protocol to evaluate all packets using the longest-match criterion. The evaluation occurs even when the destination is an unknown subnet of a known network. It changes the default behavior of the classful protocol. Instead of discarding traffic bound for unknown subnets of a known classful network, a router tries to match the largest number of bits possible against the route in its routing table. A default route matches any destination. As a last resort, the router will use the default route rather than dropping the packet. Thus, in the previous example, the **ip classless** command will cause traffic bound for 10.2.2.2 to take the default route. The **ip classless** command is on by default in Cisco IOS Software Versions 12.0 and later.

Note Routers using the longest-match criterion make routing decisions by matching the largest number of bits possible in the destination network.

Classless Routing Protocol Concepts

This topic identifies concepts of classless routing protocols.

Classless Routing Overview

Cisco.com

- **Classless routing protocols include the subnet mask with the route advertisement.**
- **Classless routing protocols support VLSM.**
- **Summary routes can be manually controlled within the network.**
- **Example of classless routing protocols are as follows:**
 - OSPF
 - EIGRP
 - RIPv2
 - IS-IS
 - BGPv4

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 2-9

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. Routing Information Protocol version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS) Protocol, and Border Gateway Protocol version 4 (BGP4) are classless routing protocols.

With classless routing protocols, different subnets within the same major network can have different subnet masks. The use of different subnet masks within the same major network is referred to as variable-length subnet masking, or VLSM. If more than one entry in the routing table matches a particular destination, the longest prefix match in the routing table is used. For example, if a routing table has different paths to 172.16.0.0/16 and to 172.16.5.0/24, packets addressed to 172.16.5.99 would be routed through the 172.16.5.0/24 path because that address has the longest match with the destination 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 route summarization process can be controlled manually and can usually be invoked at any bit position within the address. Because subnet routes are propagated throughout the routing domain, manual route summarization may be required to keep the size of the routing tables manageable.

Example

Cisco.com

A requirement for only two host addresses:
VLSM support
accommodates this

192.168.5.129 /27

E0

S1

192.168.5.209 /30

192.168.5.210 /30

E0

S0

E1

192.168.5.33 /27 192.168.5.65 /27

H465.077

- Router interfaces within the same network can have different subnet masks: VLSM is supported.
- This approach maximizes allocation of available host addresses.

© 2004 Cisco Systems, Inc. All rights reserved.

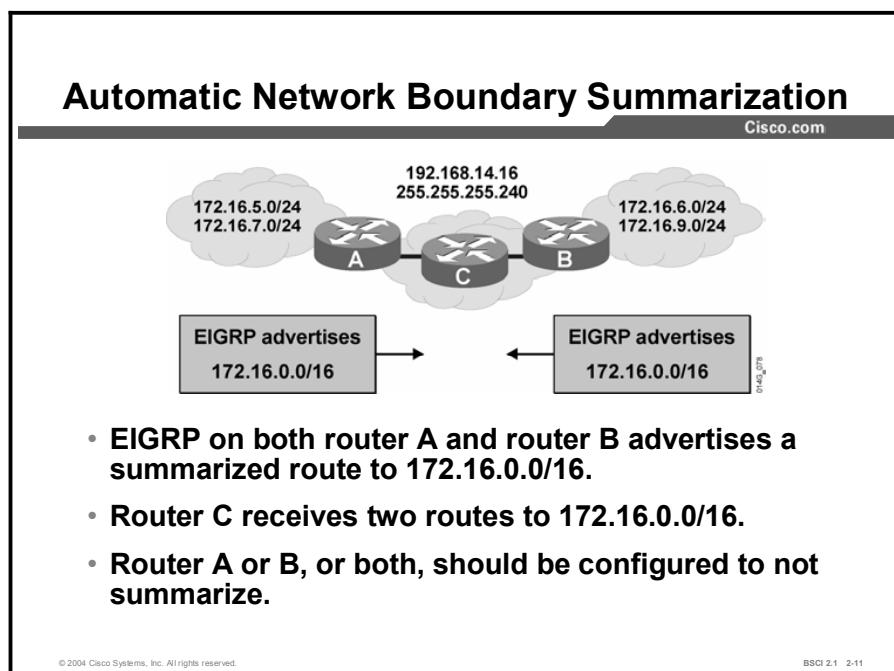
BSCI 2.1 2-10

With classful routing protocols, a consistent subnet mask must be applied to all router interfaces within the same major network, resulting in inefficient use of host addresses. Classless routing protocols allow VLSM, which enables a more appropriate allocation of address space. The subnet mask can be customized to allow the appropriate number of hosts in a network.

In the figure, the serial link is configured with a subnet mask of /30, which properly supports the point-to-point serial link requirement for only two host addresses. Meanwhile the Ethernet links are configured with a subnet mask of /27, which supports up to 30 host addresses each.

Automatic Network Boundary Summarization Using RIPv2 and EIGRP

Some classless routing protocols behave like classful ones in the way they treat the advertisement of subnets. This topic examines network summarization in those protocols.



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-11

A routing protocol that is classless does not automatically advertise every subnet. By default, classless routing protocols, such as RIPv2 and EIGRP, perform automatic network summarization at classful boundaries, just like a classful protocol does. Automatic summarization enables RIPv2 and EIGRP to be backward compatible with their predecessors, Routing Information Protocol version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP).

The difference between these protocols and their predecessors is that you can manually turn off automatic summarization. To turn off automatic summarization, use the **no auto-summary** command under the routing process. This command is not needed when you are using OSPF or IS-IS because neither protocol performs automatic network summarization by default.

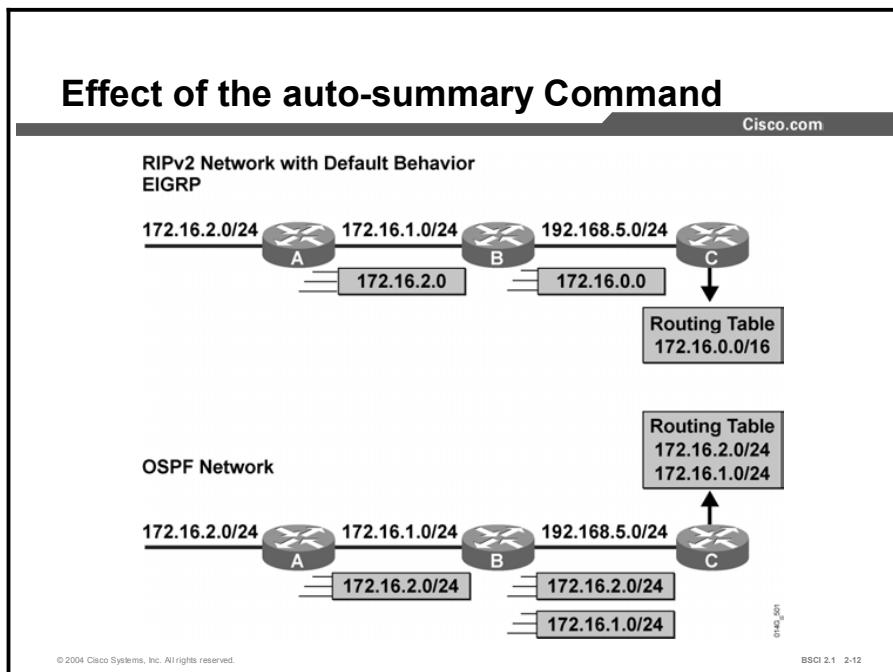
Example

The automatic summarization behavior can cause problems in a network that has discontiguous subnets or if some of the summarized subnets are unreachable via the advertising router. If a summarized route indicates that certain subnets are reachable via a router, when in fact those subnets are discontiguous or unreachable via that router, the network may have problems similar to those caused by a classful protocol. For example, in the figure, both router A and router B are advertising a summarized route to 172.16.0.0/16. Router C therefore receives two routes to 172.16.0.0/16 and cannot identify which subnets are attached to which router.

You can resolve this problem by disabling automatic summarization when running RIPv2 or EIGRP. Classless routers use the longest prefix match when selecting a route from the routing table; therefore, if one of the routers advertises without summarizing, the other routers would see subnet routes as well as the summary route. The other routers could then select the longest prefix match and follow the correct path. For example, in the preceding figure, if router A continues to summarize to 172.16.0.0/16 and router B is configured not to summarize, then router C would receive explicit routes for 172.16.6.0/24 and 172.16.9.0/24 along with the summarized route to 172.16.0.0/16. All traffic for router B subnets would be sent to router B, while all other traffic for the 172.16.0.0 network would be sent to router A. This treatment of traffic would apply for any other classless protocol.

The auto-summary Command for RIPv2 and EIGRP

This topic examines the behavior of the **auto-summary** command in various routing protocols. It contrasts the effects of the **auto-summary** command and the **no auto-summary** command.



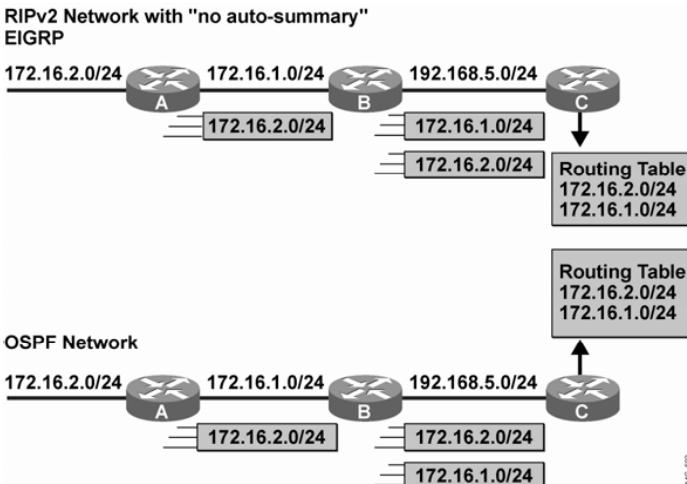
The default behavior for RIPv2, EIGRP, and BGP is to summarize networks at major classful boundaries, even though the subnet mask information is contained in routing updates.

In the RIPv2 network illustration, router B is attached to subnet 172.16.1.0/24. Therefore, if router B recognizes any network on this interface that is also a subnet of the 172.16.0.0 network, it will correctly apply the subnet mask of 255.255.255.0 to that recognized network.

However, notice how router C, which is attached to router B via the 192.168.5.0/24 network, handles routing information about network 172.16.0.0. Router B automatically summarized the 172.16.1.0/24 and 172.16.2.0/24 subnets to 172.16.0.0 before sending the route to router C, because it was sent over an interface in a different network. Rather than using the subnet mask known to router B (/24), router C applied the default classful mask for a Class B address (/16) when it received information about 172.16.0.0.

Effect of the no auto-summary Command (Cont.)

Cisco.com



In the OSPF network illustration, router B passes the subnet and subnet mask information to router C, and router C puts the subnet details into its routing table. Router C does not need to use default classful masks for the received routing information because the subnet mask is included in the routing update, and OSPF does not automatically summarize networks.

When automatic summarization is disabled, RIPv2, EIGRP, and BGP forward subnet information, even over interfaces belonging to different major networks. In the figure, automatic summarization has been disabled. Notice that now the routing table is the same for both the RIPv2 and the OSPF routers.

Example

Use the following example to disable automatic summarization in RIP:

```
router(config)# router rip
router(config-router)# version 2
router(config-router)# no auto-summary
```

Use the following example to disable automatic summarization in EIGRP and BGP:

```
router(config)# router eigrp [as #]
router(config)# router bgp autonomous-system-number
router(config-router)# no auto-summary
```

Characteristics of RIPv1

RIP is a distance vector routing protocol. This topic describes the features of RIPv1.

Characteristics of RIP Version 1

Cisco.com

- Maximum 6 paths (default = 4)
- Hop-count metric selects the path
- Routes update every 30 seconds
- Classful, no VLSM support
- Broadcast updates
- No authentication support

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-14

RIPv1 is described in RFC 1058. Key characteristics of RIPv1 include:

- 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 by default.

RIPv1 is a classful routing protocol that does not send the subnet mask in its updates. Therefore, RIPv1 does not support VLSM.

Characteristics and Configuration of RIPv2

This topic describes the characteristics of RIPv2 and provides configuration information.

Characteristics of RIPv2

Cisco.com

RIPv2 is the same as RIPv1 with the following exceptions:

- **Defined in RFC 1721, 1722, and 2453**
- **Is a classless routing protocol**
- **Multicasts rather than broadcasts updates**
- **Sends mask in the update and therefore supports VLSM**
- **Supports manual route summarization**
- **Supports Message Digest 5 (MD5) or clear text authentication**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-15

RIPv2 is a classless distance vector protocol, defined in RFCs 1721, 1722, and 2453. The purpose of RIPv2 is to update and enhance the RIPv1 protocol. The most significant addition to RIPv2 is the inclusion of the mask in the RIPv2 routing update packet. By sending the mask, RIPv2 has the following capabilities:

- Classless routing
- VLSM
- Manual route summarization

Additionally, RIPv2 uses multicast addressing for more efficient periodic updating on each interface. RIPv2 uses the 224.0.0.9 multicast address to advertise to other RIPv2 routers. This approach is more efficient because when RIPv1 uses a 255.255.255.255 broadcast address, all devices including PCs and servers will process this packet. They will perform the checksum on the Layer 2 packet and pass it up their IP stack. IP will send the packet to the User Datagram Protocol (UDP) process, and UDP will check to see if RIP port 520 is available. Most PCs and servers will not have any process running on this port and will discard the packet. RIP can fit up to 25 networks and subnets in each update, and updates are dispatched every 30 seconds. If the routing table had 1000 subnets, 40 packets would be dispatched every 30 seconds (80 packets a minute). With each packet being a broadcast, all devices must look at it; most of the devices will discard the packet.

The IP multicast address for RIPv2 has its own multicast MAC address. Devices that can distinguish between a multicast and a broadcast at the MAC layer read the start of the Layer 2 frame and determine that the destination MAC address is not for them. They can then discard all these packets at the interface level and not use CPU resources or buffer memory for these unwanted packets. Even on devices that cannot distinguish between broadcast and multicast at

Layer 2, the worst that will happen is that the RIP updates will be discarded at the IP layer instead of being passed to UDP, because those devices are not using the 224.0.0.9 address.

Security was added between RIP routers using message-digest or clear-text authentication and is implemented at the interface configuration mode. Security features are not covered in this course.

Note RIP is sometimes used as a gateway discovery technique in TCP/IP services, such as UNIX and Windows.

RIPv2 Configuration Commands

Cisco.com

```
Router(config)# router rip
```

- Starts the RIP routing process, version 1 by default

```
Router(config-router)# version 2
```

- Defines RIPv2 on the router

```
Router(config-router)# network network-number
```

- Selects participating attached networks
- Requires a major classful network number

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 2-16

By default, the Cisco IOS software receives both RIPv1 and RIPv2 packets; however, it sends only RIPv1 packets. To configure the software to send and receive packets from only one version, use the **version {1 | 2}** command.

Regardless of the version, a **network** command is required under the RIP routing process using the classful network number.

RIPv2 Configuration Commands (Cont.)

Cisco.com

```
Router(config-if)# ip rip send | receive version  
1 | 2 or 1 2
```

- Interface command that specifies which version of RIP will be sent and received on an individual interface basis

```
Router(config-if)# ip summary-address rip network  
mask
```

- Enables manual summarization of RIP routes on a per-interface basis
- Disable autosummarization with the no auto-summary command under RIP

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-17

Although the RIP **version** command controls the overall default behavior of RIP, it may be necessary to control the version of RIP on a per-interface basis. To control the version of RIP on each interface, use the **ip rip send version** and **ip rip receive version** interface commands. Version control per interface may be required when you are connecting legacy RIP networks to newer networks.

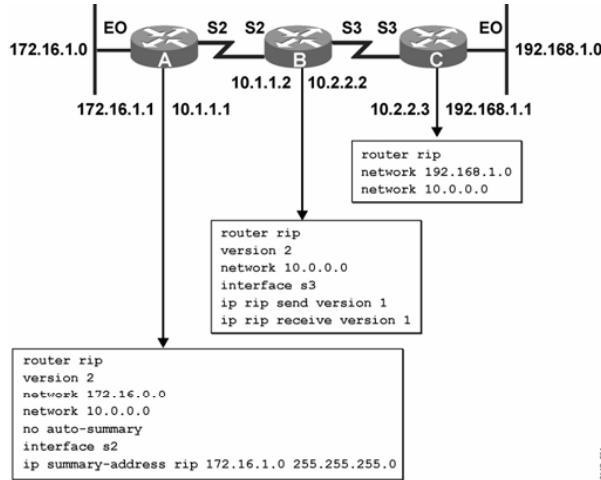
By default, automatic summarization across network boundaries is activated for all networks in both versions of RIP. Manually summarizing routes in RIPv2 improves scalability and efficiency in large networks. The more specific routes are not advertised, only the summary routes, thus reducing the size of the IP routing table and allowing the router to handle more routes.

Networks are automatically summarized at their classful boundaries. Manual summarization is done at the interface. One limitation of RIPv2 is that routes can be summarized only up to the classful network boundary. RIPv2 does not support classless interdomain routing (CIDR)-type summarization to the left of the classful boundary. To summarize RIP routes on nonclassful boundaries, do the following:

- Turn off autosummarization using the **no auto-summary** command under the RIP process.
- Use the **ip summary-address rip** interface command and define a network number and mask that meet the particular requirement.

RIPv2 Configuration Example

Cisco.com



The figure illustrates how RIPv1 and RIPv2 coexist in the same network. Router A is running RIPv2, and router C is running RIPv1. Router B runs both versions of RIP to bring the two versions together. Notice that the **ip rip send version 1** and **ip rip receive version 1** commands are required only on interface serial 3 of router B, because RIPv2 is configured as the primary version for all interfaces. The serial 3 interface has to be manually configured to support RIPv1 so it can connect correctly with router C.

The **ip summary-address rip** command is configured on router A with the **no auto-summary** option. The combination of these two commands allows router A to send the 172.16.1.0 subnet detail to router B. Because router B is in a different network (10.0.0.0), the default behavior for router A is to send only the classful summarization (172.16.0.0) to router B.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Interpret classful routing tables using the **show ip route** command
- Classless routing protocols include **RIPv2, EIGRP, OSPF, IS-IS, and BGPv4**.
- Classless routing protocols support **VLSM** and manual summarization.
- The **no auto-summary** command turns off automatic summarization.
- **RIPv1** supports a simple metric with a periodic update. It is classful and does not support VLSM.
- **RIPv2** supports classless routing, VLSM, manual route summarization, multicast routing updating, and RIPv2 packet authentication.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-19

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 characteristics describe classful routing protocols? (Choose two.)
- A) They carry the subnet mask in the routing updates.
 - B) RIPv1 and IGRP are examples.
 - C) They do not carry the subnet mask in the routing updates.
 - D) Subnets of the same major network use a variety of subnet masks.
- Q2) Where do classful routing protocols perform automatic network summarization?
- A) at locations configured by an administrator
 - B) at any bit boundary desired
 - C) across major network boundaries
 - D) none of the above
- Q3) By default, where does a router running a classful routing protocol send traffic bound for unknown subnets of a major network that is in the routing table?
- A) to the network that best matches the route
 - B) to the default route
 - C) back to the sender
 - D) nowhere—discards the packets
- Q4) What is the command to change the default classful lookup behavior?
- A) **ip forward protocol**
 - B) **ip classless**
 - C) **no ip classful**
 - D) **ip routing**
- Q5) Which three protocols are classless routing protocols? (Choose three.)
- A) EIGRP
 - B) IGRP
 - C) OSPF
 - D) RIPv2
 - E) RIPv1

- Q6) Which two protocols summarize to major network boundaries by default? (Choose two.)
- A) OSPF
 - B) EIGRP
 - C) IS-IS
 - D) RIPv2
- Q7) What must you do to configure a router running EIGRP so that it advertises subnets across a classful network boundary?
- A) nothing—classless protocol that does not automatically summarize
 - B) give the **ip classless** command
 - C) give the **no auto-summary** command
 - D) nothing—no way to accomplish this type of configuration
- Q8) Which two characteristics are 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 perform load balancing over six equal-cost paths.
 - E) It multicasts updates every 30 seconds.
- Q9) Which two commands are required when configuring route summarization in RIPv2? (Choose two.)
- A) **network** command with summarized mask
 - B) **no auto-summary** under the routing process
 - C) **ip rip send version 2** on the interface
 - D) **ip summary-address rip** on the interface
- Q10) The default behavior of RIP is to send version 1 updates and receive both version 1 and version 2 updates.
- A) true
 - B) false

Quiz Answer Key

- Q1) B, C
Relates to: Classful Routing Protocol Concepts
- Q2) C
Relates to: Automatic Network Boundary Summarization in a Classful Routing Protocol
- Q3) D
Relates to: Examining a Classful Routing Table
- Q4) B
Relates to: Examining a Classful Routing Table
- Q5) A, C, D
Relates to: Classless Routing Protocol Concepts
- Q6) B, D
Relates to: Automatic Network Boundary Summarization Using RIPv2 and EIGRP
- Q7) C
Relates to: The auto-summary Command for RIPv2 and EIGRP
- Q8) B, D
Relates to: Characteristics of RIPv1
- Q9) A, B, D
Relates to: Characteristics and Configuration of RIPv2
- Q10) B, D
Relates to: Characteristics and Configuration of RIPv2

IP Routing Protocol Comparison

Overview

Each IP routing protocol has its own unique characteristics. These protocols also share characteristics with other protocols. This lesson compares and contrasts the various IP routing protocols. This lesson also illustrates the qualities of IP routing protocols, such as administrative distance and floating static routes.

Relevance

An important task for network administrators is determining the appropriate protocol to use and then configuring it properly. A network runs smoothly and efficiently when you use the correct routing protocols with the correct configuration. To choose the correct protocols, you must understand their differences and similarities.

Objectives

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

- Describe administrative distance in terms of routing protocols
- Explain floating static routes
- List the requirements for inserting routes into the IP routing table
- Discuss the routing protocol comparison charts

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

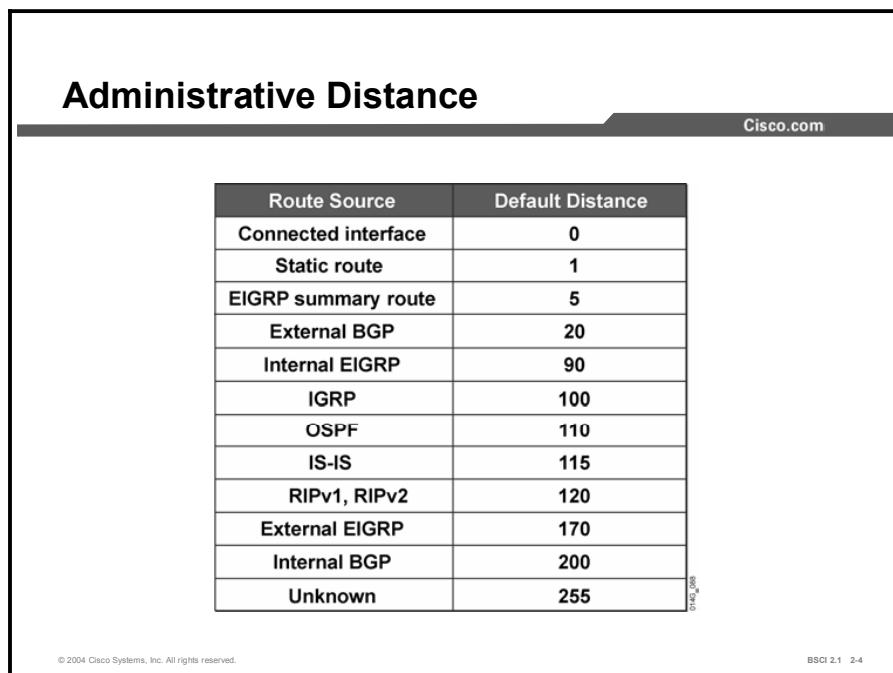
Outline

Cisco.com

- **Overview**
- **Administrative Distance**
- **Floating Static Routes**
- **Criteria for Inserting Routes in the IP Routing Table**
- **Comparing Routing Protocol Charts**
- **Summary**
- **Quiz**

Administrative Distance

Cisco routers use administrative distance when using more than one routing protocol. This topic describes the concept and use of administrative distance in terms of routing protocols.



The figure shows a table titled "Administrative Distance" from Cisco.com. The table lists various route sources and their corresponding default administrative distances. The columns are "Route Source" and "Default Distance". The rows include: Connected interface (0), Static route (1), EIGRP summary route (5), External BGP (20), Internal EIGRP (90), IGRP (100), OSPF (110), IS-IS (115), RIPv1, RIPv2 (120), External EIGRP (170), Internal BGP (200), and Unknown (255). The table has a dark header row and light gray rows for the data.

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1, RIPv2	120
External EIGRP	170
Internal BGP	200
Unknown	255

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-4

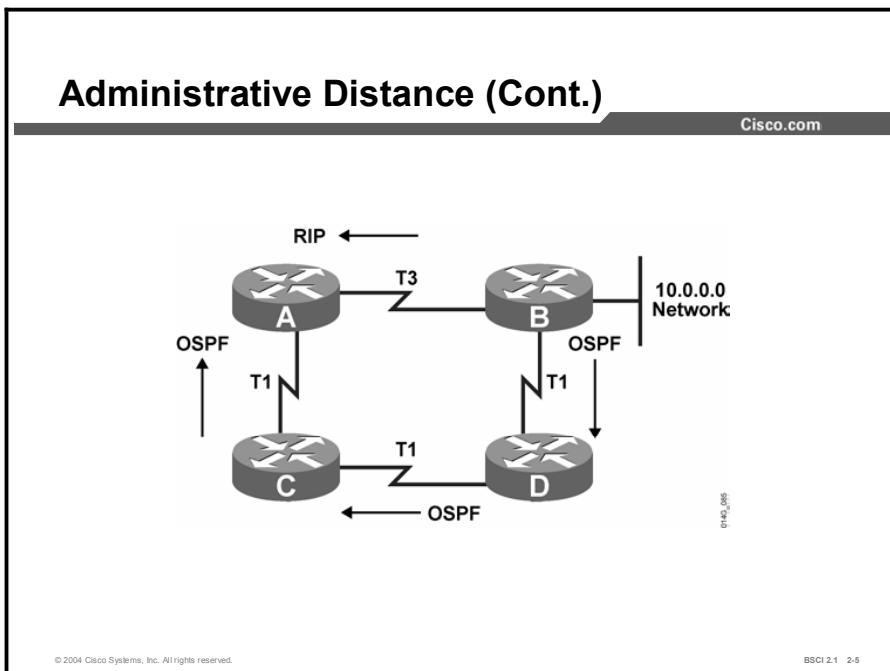
Most routing protocols have metric structures and algorithms that are not compatible with other protocols. It is critical for a network using multiple routing protocols to have seamless exchange of route information and the ability to select the best path across multiple protocols. Cisco routers use a value called administrative distance to select the best path when they learn two or more routes to the same destination from different routing protocols.

Administrative distance rates the *believability* of a routing protocol. Cisco has assigned a default administrative distance value to each routing protocol supported on its routers. Each routing protocol is prioritized in the order of most believable to least believable. Some examples of prioritization are as follows:

- Prefer manually configured routes (static routes) to dynamically learned routes
- Prefer protocols with sophisticated metrics to protocols with more deterministic metrics
- Prefer External Border Gateway Protocol (EBGP) over most other dynamic protocols

In the figure, the table lists the default administrative distance of the protocols supported by Cisco routers. The administrative distance is a value between 0 and 255. The lower the administrative distance value, the higher the reliability of the protocol.

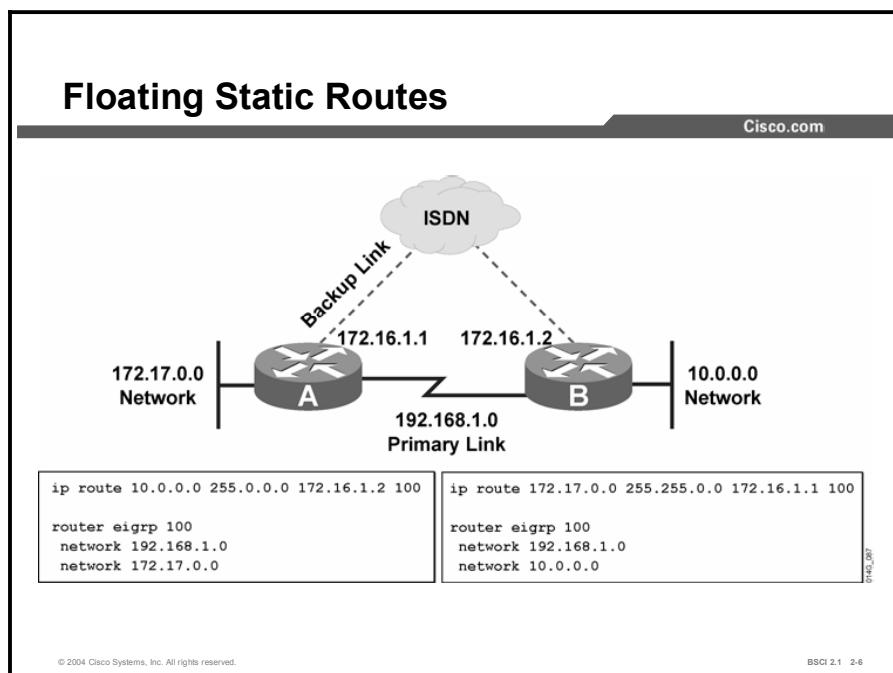
Example



For example, if router A receives a route to network 10.0.0.0 from RIP and receives a route to the same network from OSPF, the router compares the administrative distance of RIP, 120, with the administrative distance of OSPF, 110. The router uses the administrative distance value to determine that OSPF is more reliable and adds the OSPF version of the route to the routing table.

Floating Static Routes

The topic explains how to use administrative distance to create floating static routes.



Based on administrative distance, routers believe static routes over any dynamically learned route. A directly connected interface is the only default administrative distance lower than that of a static route. There may be times when the default behavior is not the desired behavior.

When you have configured a static route as a backup to a dynamically learned route, the static route should not be used as long as the dynamic route is available. First, consider that the syntax for configuring a static route is **ip route prefix mask address/interface [distance]**.

The optional administrative distance value in this command can be manipulated to make the static route appear less desirable. Administrative distance can also be manipulated to make one static route appear less desirable than another static route. A static route that appears in the routing table only when the primary route goes away is called a floating static route.

Note It is important to remember that the lower the administrative distance, the more reliable the protocol is assumed to be.

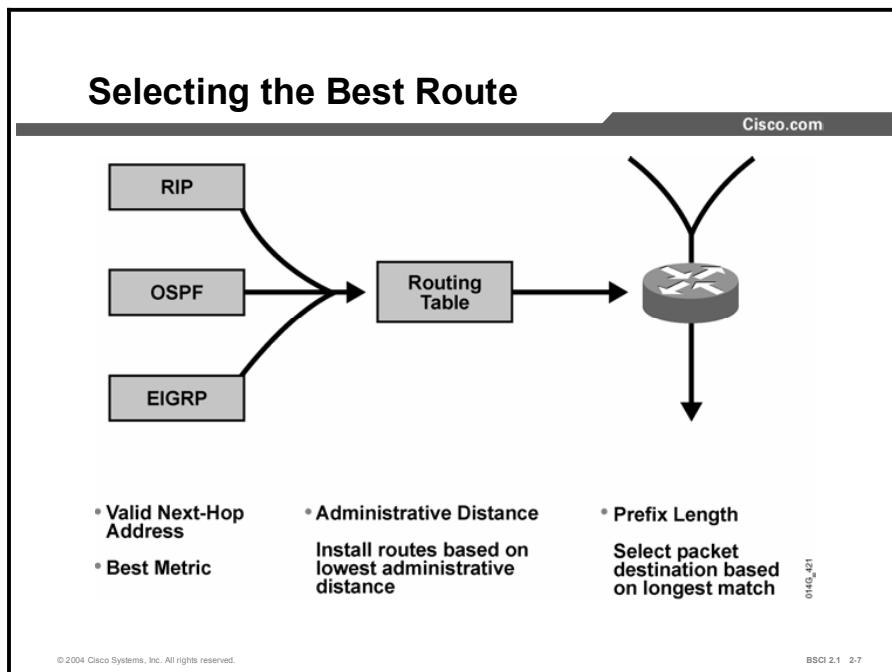
Example

In the preceding figure, routers A and B have two connections—a point-to-point serial connection that is the primary link and an ISDN link to be used if the other line goes down. Both routers use EIGRP but do not route the ISDN 172.16.1.0 network link.

A static route has been created on each router pointing to the ISDN interface of the other router. Because EIGRP has an administrative distance of 90, the static route has been given an administrative distance of 100. As long as router A has an EIGRP route to the 10.0.0.0 network, it appears more believable than the static route, and the EIGRP route is used. If the serial link goes down and disables the EIGRP route, router A inserts the static route into the routing table. A similar process happens on router B with its route to the 172.17.0.0 network.

Criteria for Inserting Routes in the IP Routing Table

This topic details the selection process that the router uses for inserting routes in the IP routing table.



One of the intriguing aspects of Cisco routers is the way the router chooses the best route among those presented by routing protocols, manual configuration, and various other means. Although route selection is not difficult, to understand it completely requires some knowledge about the way Cisco routers work. The router must consider the following four criteria:

- **Valid next-hop IP address:** As each routing process receives updates and other information, the router first verifies that the route has a valid next-hop IP address.
- **Metric:** If the next hop is valid, then the routing protocol chooses the best path to any given destination based on the lowest metric. The routing protocol attempts to install this path into the routing table. For example, if EIGRP learns of a path to 10.1.1.0/24 and decides that this particular path is the best EIGRP path to this destination, then the routing protocol tries to install the learned path into the routing table.
- **Administrative distance:** The next consideration is administrative distance. If more than one route exists for the same network, the router decides which route to install based on the administrative distance of the source of the route. If the routing protocol that is presenting the path to a particular destination has the lowest administrative distance compared to the other ways the router has learned about this network, then the router installs the route in the routing table. If that route does not have the best administrative distance, the route is rejected.

- **Prefix:** The router looks at the prefix being advertised. If there is no exact match to that prefix in the routing table, the route is installed. For example, the router has three routing processes running on it, and each process has received these following routes:
 - EIGRP (internal): 192.168.32.0/26
 - RIP: 192.168.32.0/24
 - OSPF: 192.168.32.0/19

Because each route has a different prefix length, also known as the subnet mask, the routes are considered different destinations and are installed in the routing table.

Comparing Routing Protocol Charts

This topic presents charts that are helpful when you are comparing routing protocols.

Protocols, Ports, and Reliability

Cisco.com

Routing Protocol	Protocol No.	Port No.	Update Reliability
IGRP	9		Best-effort delivery
EIGRP	88		1-to-1 window
OSPF	89		1-to-1 window
RIP		UDP 520	Best-effort delivery
BGP		TCP 179	Uses TCP windowing

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 2-8
0145_380

IGRP, EIGRP, and OSPF are transport-layer protocols that run directly over IP. IGRP uses connectionless delivery for its routing updates. Routers receiving IGRP updates do not need to acknowledge the receipt of these updates. EIGRP and OSPF have more reliability built into their update processes. They both require the acknowledgment of one update before they send another. Thus, they have a 1-to-1 window—one update and one acknowledgement.

RIP and BGP both reside at the application layer. RIP uses UDP as its transport protocol; its updates are sent unreliable with best-effort delivery.

BGP uses TCP as its transport protocol. It takes advantage of the reliability mechanisms and windowing of TCP, which is important when you consider the number of routes a BGP router sends in its updates. BGP routers often carry well over 100,000 routes in their routing tables. If OSPF or EIGRP had to send updates for 100,000 routes with their 1-to-1 window, it would take a long time. Even if information for 100 routes could fit in one update, it would still take 1000 updates to send the entire table. Each update would have to be acknowledged before another could be sent. On the other hand, BGP routers using TCP have a 65,536-byte window limit for their updates. The routers can send information with many more routes in each update than either OSPF or EIGRP.

Note IS-IS is a network-layer protocol and does not use the services of IP to carry its routing information. IS-IS packets are encapsulated directly into a data-link layer frame.

Routing Protocol Comparison Chart

Cisco.com

Characteristic	RIPv2	EIGRP*	IS-IS	OSPF	BGP**
Distance vector	X	X			X
Link state			X	X	
Hierarchical topology required			X	X	
Automatic route summarization	X	X			X
Manual route summarization	X	X	X	X	X
VLSM support	X	X	X	X	X
Classless	X	X	X	X	X
Metric	Hops	Comp	Cost	Cost	Path Attributes
Convergence time	Slow	VryFst	Fast	Fast	Slow

* EIGRP is an advanced distance vector protocol with some characteristics also found in link-state protocols.

** BGP is a path-vector protocol

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-9

RIPv2 is a distance-vector protocol, but it is classless and supports VLSM. RIPv2 automatically summarizes routes at major classful network boundaries; however, summarization can be disabled and some manual summarization is possible. RIPv2 uses hop count, the number of routers between the router and the destination network, as its metric. The maximum allowable hop count is 15. RIP uses timers to prevent loops, but these also slow network convergence.

EIGRP is an advanced distance-vector routing protocol; however, it demonstrates some of the same characteristics as link-state protocols, such as maintaining a topological table and neighbor relationships. EIGRP automatic route summarization is enabled by default, but you can disable it and configure manual route summarization. EIGRP uses a composite metric: bandwidth and delay by default. Although hop count is not part of the composite metric, EIGRP has a maximum hop count of 255 (the default is 100). EIGRP generally has the fastest convergence time, because it maintains a feasible successor, which is a backup route, in its topology table. If the best path fails, EIGRP immediately switches to the feasible successor without performing additional best-path calculations.

OSPF and IS-IS are both classless, link-state protocols that support VLSM. They require a hierarchical topology with a backbone that carries interarea traffic. OSPF and IS-IS use the Dijkstra shortest path first (SPF) algorithm for calculating the best paths through the network. They use cost as their metric. The cost of OSPF is based on bandwidth in Cisco routers. The IS-IS cost metric has a maximum value of 1023, and Cisco uses a default value of 10 for all types of WAN and LAN links. With OSPF and IS-IS, route summarization must be manually configured. Network convergence after a topology change is fairly fast because routers already recognize all the links within their area.

BGP is a classless routing protocol that keeps track of paths to autonomous systems. It automatically summarizes routes at major classful network boundaries; however, you can disable summarization and configure manual summarization under the routing protocol. It has a highly complicated metric based on a prioritized evaluation of the attributes of each path. Convergence time is not an important issue with BGP; reliability is a much greater concern.

Comparison of Default Timers

Cisco.com

Protocol	Update Frequency	Hello Frequency	Other Timers
RIP	30 sec plus triggered	NA	Hold & invalid—180 sec flush—240
IGRP	90 sec plus triggered	NA	Hold—280 sec invalid—270, flush—630
EIGRP	Triggered	60 sec—multipoint T1 or less, 5 sec—others	Hold—180 sec multipoint T1 or less, 15 sec—others (3 x hello interval)
IS-IS	Triggered, plus LS database synchronized on LAN every 10 sec and at startup on PTP	10 sec	Hold—30 sec
OSPF	Triggered, plus LSAs flooded every 30 min	30 sec—NBMA, 10 sec—others	Dead—120 sec NBMA, 40 sec others (4 x hello interval)
BGP	Triggered	60 sec	Hold—180 sec

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 2-10
0746-119

All routing protocols use timers, which have default values. Distance vector protocols send their routing updates on a regular basis. Distance vector protocols use routing updates to maintain neighbor relationships. The protocols send the entire routing table, subject to the rules of split horizon. RIP sends updates every 30 seconds; IGRP sends updates every 90 seconds. The update interval affects the holddown for these protocols. Holddown, invalid, and flush times are as follows:

- **Holddown:** An interval, in seconds, during which routing information regarding a worse or equivalent metric path is suppressed. It should be at least three times the value of the *update* argument. A route enters a holddown (possibly down) state when it receives an update packet that indicates an unreachable route. The route is marked inaccessible and advertised as unreachable. However, the route is still used to forward packets. When holddown expires, routes advertised by other sources with a worse or equivalent metric are accepted and the route is no longer inaccessible. The default is 180 seconds.
- **Invalid:** An interval of time, in seconds, after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a holddown state. The route is marked inaccessible and advertised as unreachable. However, the route still forwards packets. The default is 180 seconds.
- **Flush timer:** An amount of time, in seconds, that must pass before the route is removed from the routing table; the interval that is specified should be greater than the value of the *invalid* argument. If it is less than the value of the *invalid* argument, the proper holddown interval cannot elapse, which results in acceptance of a new route before the holddown interval expires. The default is 240 seconds.

Protocols that do not regularly advertise their routing tables—EIGRP, IS-IS, OSPF, and BGP—must have some way of establishing and maintaining neighbor relationships. EIGRP, IS-IS, OSPF, and BGP establish and maintain neighbor relationships by exchanging hello packets on a regular basis. For EIGRP and OSPF, the hello interval varies by the type of link between the two neighboring routers. Faster links receive more frequent hellos.

Link-state protocols refresh the link-state database at intervals, even if there have been no link-state changes, to ensure that the information has not become corrupted while in a database. With OSPF, when a link-state advertisement (LSA) is 30 minutes old, the router originating the LSA refloods the information. With IS-IS, the link-state database on a LAN link is synchronized every 10 seconds with a multicast complete sequence number protocol data unit (CSNP). On point-to-point links, this synchronization is done at startup.

These protocols use *hold time*, which is different from *holddown* for distance-vector protocols. If a router does not receive a hello packet from a neighbor within the specified hold time, that neighbor is down and routes through that neighbor are unavailable. For OSPF, the equivalent term is dead interval.

All of these timers can be configured or defaulted. For example, the default values for the hold time and dead interval depend on the frequency of hellos, but they are generally three to four times the hello value. For some applications, three to four times the hello value may not be an appropriate value.

A network administrator should consider several issues before changing the default timers. You must not set hold timers so low that neighbor relationships are torn down unnecessarily. On the other hand, longer hold times may delay network convergence. This delay is due to the long down time for a router before the hold timer of the neighbor expires and it notices the topology change. Similarly, the smaller the hello interval, the faster the topological changes are detected, although more routing traffic ensues.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Cisco routers use administrative distance to rate the believability of a routing protocol.
- By default, static routes are believed over any dynamically learned route, based on administrative distance.
- Cisco routers select the best route based on four criteria:
 - Valid next-hop IP address
 - Metric
 - Prefix
 - Administrative distance
- Each routing protocol has distinct characteristics.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 2-11

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-1: Migrating to a Classless Routing Protocol

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) If a router learns paths to a destination network from both OSPF and EIGRP, which path does it put into the routing table based on administrative distance?
- A) route learned from OSPF
 - B) route learned from EIGRP
 - C) load balances between them
- Q2) What must you do to configure a floating static route?
- A) Configure a static route with an administrative distance lower than the administrative distance of the routing protocol.
 - B) Configure a static route with an administrative distance higher than the administrative distance of the routing protocol.
 - C) Use the special keyword **floating** at the end of the **static route** command.
- Q3) What four criteria does a router consider when choosing a route to install in the routing table? (Choose four.)
- A) the metric—the path with the highest metric
 - B) the metric—the path with the lowest metric
 - C) the administrative distance—the source with the highest value
 - D) the administrative distance—the source with the lowest value
 - E) the default subnet mask of the route
 - F) whether or not the next-hop address is reachable
 - G) the exact prefix being advertised
- Q4) Which three routing protocols are transport-layer protocols? (Choose three.)
- A) IGRP
 - B) BGP
 - C) EIGRP
 - D) OSPF
- Q5) Which two routing protocols are link-state protocols? (Choose two.)
- A) EIGRP
 - B) BGP
 - C) OSPF
 - D) IS-IS

Quiz Answer Key

Q1) B

Relates to: Administrative Distance

Q2) B

Relates to: Floating Static Routes

Q3) B, D, F, G

Relates to: Criteria for Inserting Routes in the IP Routing Table

Q4) A, C, D

Relates to: Comparing Routing Protocol Charts

Q5) C, D

Relates to: Comparing Routing Protocol Charts

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:

- Quiz 2-1: IP Routing Overview
- Quiz 2-2: Characteristics of Routing Protocols
- Quiz 2-3: IP Routing Protocol Comparison

Quiz 2-1: IP Routing Overview

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

Objectives

This assessment tests your knowledge of how to:

- Explain the principles of static routing
- Configure static routing
- Describe the principles of dynamic routing
- Discuss the principles of On-Demand Routing
- Configure On-Demand Routing

Quiz

Answer these questions:

- Q1) In which protocol does the network statement tell the router which networks to advertise, not which interfaces participate in the routing process?
- A) OSPF
 - B) IS-IS
 - C) EIGRP
 - D) BGP
- Q2) Which routing protocol does not use the network statement?
- A) OSPF
 - B) IS-IS
 - C) EIGRP
 - D) BGP
- Q3) Which command will create a static default route?
- A) `ip route 0.0.0.0 0.0.0.0 192.168.1.1`
 - B) `ip route 0.0.0.0 255.255.255.255 192.168.1.1`
 - C) `ip route 255.255.255.255 0.0.0.0 192.168.1.1`
 - D) `ip route 0.0.0.0 192.168.1.1`
- Q4) Which two routing protocols enable you to use the network statement to specify exactly which interfaces participate in the protocol, rather than require the major classful network to be specified? (Choose two.)
- A) RIP
 - B) EIGRP
 - C) IS-IS
 - D) OSPF

- Q5) Which two types of routes can be present in the routing table of a router? (Choose two.)
- A) static
 - B) multipoint
 - C) distance-linkstate
 - D) dynamic
- Q6) The networks listed in the network statements for an OSPF router are:
- A) all the networks the router needs to recognize
 - B) remote networks only
 - C) directly connected networks only
 - D) none of the above
- Q7) Which two characteristics are drawbacks to static routing? (Choose two.)
- A) It must be manually configured.
 - B) It must be manually updated when the network topology changes.
 - C) It consumes network bandwidth.
 - D) It uses more router resources.
- Q8) Which two characteristics are drawbacks to dynamic routing? (Choose two.)
- A) It must be manually configured.
 - B) It must be manually updated when the network topology changes.
 - C) It consumes network bandwidth.
 - D) It uses more router resources.
- Q9) How is routing performed by the spoke routers when using ODR?
- A) have full routes for the entire network
 - B) have routes for their connected networks and a default route pointing to the hub router
 - C) send the hub router a default route pointing to themselves
 - D) have routes to other spokes, but not to any other parts of the network
- Q10) Which protocol carries ODR information?
- A) TCP
 - B) UDP
 - C) CDP
 - D) PPP

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 90 percent or better.

Quiz 2-2: Characteristics of Routing Protocols

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

Objectives

This assessment tests your knowledge of how to:

- Describe the concepts of classful routing protocols
- Describe automatic network boundary route summarization in a classful routing protocol
- Interpret a classful routing table
- Identify concepts of classless routing protocols
- Discuss network boundary route summarization in a classless routing protocol
- Contrast the effects of **auto-summary** and **no auto-summary** options
- Describe the Routing Information Protocol version 1 method of distance vector routing
- Identify the Routing Information Protocol version 2 characteristics and configurations

Quiz

Answer these questions:

- Q1) Which two actions does the **ip classless** command cause the router to do? (Choose two.)
- A) evaluate all packets using the longest-match criterion
 - B) route to major networks only
 - C) include subnet mask information in all routing updates
 - D) send a default route to all its neighbors
- Q2) Which two characteristics are true of a classful routing protocol? (Choose two.)
- A) includes subnet mask information in its routing updates
 - B) does not include subnet mask information in its routing updates
 - C) automatically summarizes routes when advertised across major network boundaries
 - D) pays no attention to major network boundaries
- Q3) When **ip classless** is enabled, the routing table _____.
- A) has all classless routes tagged
 - B) includes routes to major classful networks only
 - C) looks the same as a routing table without **ip classless** enabled
 - D) gives a special administrative distance to subnetted routes
- Q4) What is the default subnet mask for Class A addresses?
- A) 255.0.0.0
 - B) 255.255.0.0
 - C) 255.255.255.0
 - D) no default mask for this class

- Q5) What is the default subnet mask for Class B addresses?
- A) 255.0.0.0
 - B) 255.255.0.0
 - C) 255.255.255.0
 - D) no default mask for this class
- Q6) What is the default subnet mask for Class C addresses?
- A) 255.0.0.0
 - B) 255.255.0.0
 - C) 255.255.255.0
 - D) no default mask for this class
- Q7) In a router running a classful protocol, what happens when the routing update information contains the same major network number as configured on the receiving interface?
- A) The router applies the default mask for that class of address.
 - B) The router looks further into the update packet for the subnet mask information.
 - C) The router recognizes this update as a duplicate update and discards the packet.
 - D) The router applies the same subnet mask as the one configured on its interface.
- Q8) Where does a classful routing protocol allow manual route summarization?
- A) at each interface only
 - B) under the routing protocol only
 - C) both at the interface and under the routing protocol
 - D) manual route summarization not allowed
- Q9) Which two characteristics are true of FLSM? (Choose two.)
- A) efficiently allocates IP addresses in a network
 - B) can result in IP addresses being wasted
 - C) cannot be used with classful routing protocols
 - D) means that all interfaces in a major network must use the same subnet mask
- Q10) Which two of the following protocols are classful routing protocols? (Choose two.)
- A) RIPv1
 - B) RIPv2
 - C) IGRP
 - D) EIGRP
- Q11) What is the command to disable autosummarization?
- A) **no summary-route**
 - B) **ip classless**
 - C) **no auto-summary**
 - D) **ip longest-match**

- Q12) Which four protocols support VLSM? (Choose four.)
- A) RIPv1
 - B) RIPv2
 - C) OSPF
 - D) IGRP
 - E) EIGRP
 - F) BGP4
- Q13) If you are using VLSM and more than one entry in a routing table matches the destination network, how does a router select which one to use?
- A) It uses the oldest route.
 - B) It uses the route with the longest prefix match.
 - C) It uses the route with the lowest administrative distance.
 - D) It uses the first matching route listed in the routing table.
- Q14) Which two characteristics are true of classless routing protocols? (Choose two.)
- A) The subnet mask must match on all interfaces in a major network.
 - B) The subnet mask can vary within a major network.
 - C) Subnet mask information is contained in routing updates.
 - D) Subnet mask information is not contained in routing updates.
- Q15) Which three statements are true concerning classless routing protocols? (Choose three.)
- A) Summary routes can be manually controlled within the network.
 - B) VLSM is supported.
 - C) FLSM is supported, VLSM is not.
 - D) Discontiguous subnets may not be used.
 - E) The subnet mask is included in the routing updates.
- Q16) Categorize each of these routing protocols as either a classful or classless routing protocol.

	Classful	Classless
EIGRP	_____	_____
IGRP	_____	_____
RIPv1	_____	_____
OSPF	_____	_____
IS-IS	_____	_____
RIPv2	_____	_____
BGP4	_____	_____

- Q17) Which protocol supports manual route summarization?
- A) RIPv1
 - B) IGRP
 - C) RIPv2

- Q18) Write the configuration command that sends RIPv2 on interface serial 1 only.
- A) _____ **interface serial 1**
B) _____ **ip rip send version 2**
- Q19) Which protocol supports CIDR?
- A) RIPv1
B) IGRP
C) RIPv2
- Q20) Configuring the **no auto-summary** command under RIPv2 will _____.
A) allow RIP to summarize at the classful boundary
B) allow the administrator to configure summarization at a nonclassful boundary
C) turn RIPv2 into a classless routing protocol
D) do nothing—RIPv2 will not support this command

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 70 percent or better.

Quiz 2-3: IP Routing Protocol Comparison

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

Objectives

This assessment tests your knowledge of how to:

- Describe administrative distance in terms of routing protocols
- Explain floating static routes
- List the requirements for inserting routes into the IP routing table
- Discuss the routing protocols comparison charts

Quiz

Answer these questions:

- Q1) What must you change to make a static route into a floating static route?
- A) the next-hop IP address
 - B) the administrative distance
 - C) the interface address
 - D) the metric for the route
- Q2) What is the default hello frequency for BGP?
- A) 10 seconds
 - B) 40 seconds
 - C) 60 seconds
 - D) depends on the speed of the link
- Q3) How often are RIP updates sent by default?
- A) every 10 seconds
 - B) every 30 seconds
 - C) every 90 seconds
 - D) not sent at a regular interval
- Q4) How often are EIGRP updates sent by default?
- A) every 10 seconds
 - B) every 30 seconds
 - C) every 90 seconds
 - D) updates triggered by topology changes
- Q5) Which of the following routing protocols can perform manual route summarization?
- A) RIPv2
 - B) EIGRP
 - C) OSPF
 - D) BGP
 - E) all of the above

- Q6) What port number does BGP use?
- A) TCP port 179
 - B) UDP port 23
 - C) UDP port 90
 - D) TCP port 65
- Q7) How many routing updates can EIGRP send before it expects an acknowledgment?
- A) one
 - B) three
 - C) four
 - D) depends on the speed of the link
- Q8) If a router discovers paths to the same network from different routing sources, how does it determine which to believe?
- A) It takes the protocol whose route has the best metric.
 - B) It evaluates the age of the routing information.
 - C) The router always prefers Cisco proprietary routing protocols.
 - D) It uses the route from the source with the lowest administrative distance.
- Q9) If both OSPF and IS-IS are trying to install a route to the same network in the routing table, which does the router choose based on administrative distance?
- A) OSPF
 - B) IS-IS
 - C) neither
- Q10) What is the metric used by OSPF?
- A) hop count
 - B) composite metric
 - C) cost
 - D) path attributes

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 2-1: IP Routing Overview

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

Quiz 2-2: Characteristics of Routing Protocols

- Q1) A, C
- Q2) B, C
- Q3) C
- Q4) A
- Q5) B
- Q6) C
- Q7) D
- Q8) D
- Q9) B, D
- Q10) A, C
- Q11) C
- Q12) B, C, E, F
- Q13) B
- Q14) B, C
- Q15) A, B, E
- Q16) Classful Classless
 - EIGRP _____ X_____
 - IGRP X_____ _____
 - RIPv1 X_____ _____
 - OSPF _____ X_____
 - IS-IS _____ X_____
 - RIPv2 _____ X_____
 - BGP4 _____ X_____
- Q17) C
- Q18) **interface serial 1
ip rip send version 2**
- Q19) C
- Q20) C

Quiz 2-3: IP Routing Protocols Comparison

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

Module 3

Configuring EIGRP

Overview

In present-day and future routing environments, Enhanced Interior Gateway Routing Protocol (EIGRP) offers benefits and features over historical distance-vector routing protocols like Routing Information Protocol version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP). These benefits include rapid convergence, lower bandwidth utilization, and multiple routed protocol support (IP, Internet Packet Exchange [IPX], and AppleTalk).

EIGRP uses three databases in the path selection process: the EIGRP neighbor table, the EIGRP topology table, and the IP routing table. The neighbor table contains a list of directly connected EIGRP routers that have established an adjacency with a given router. The topology table includes route entries for all destinations that the router has learned. EIGRP chooses the best successor routes to a destination from the topology table and places these routes in the routing table.

EIGRP supports five packet types: hello, update, query, reply, and acknowledgment (ACK). Fields in the hello packet build adjacencies between EIGRP neighbors. The Cisco IOS software **debug** and **show** commands are used to troubleshoot EIGRP neighbor adjacency problems.

The EIGRP Diffusing Update Algorithm (DUAL) finite state machine embodies the decision process for all route computations. DUAL tracks all routes advertised by all EIGRP neighbors and then uses a formula to calculate the best route.

A basic EIGRP configuration contains a default network and uses the wildcard option for the network statement. The Cisco IOS **show** commands can be used to troubleshoot EIGRP configuration problems. Advanced configuration options for EIGRP include manual route summarization, unequal path-cost load balancing, and limiting EIGRP bandwidth utilization on WAN links.

EIGRP is scaled in large and growing internetworks by using two methods to perform query scoping, which limits the range of EIGRP queries. The two methods are effective route summarization and the EIGRP **stub** command.

Module Objectives

Upon completing this module, you will be able to implement an effective scalable network, given Enhanced Interior Gateway Routing Protocol-specific design and configuration techniques.

Module Objectives

Cisco.com

- **EIGRP as an internetwork routing protocol**
- **Describe how EIGRP operates and verify EIGRP connectivity and operation**
- **Describe how EIGRP DUAL selects a successor or feasible successor**
- **Configure and verify basic EIGRP**
- **Configure EIGRP with advanced options to implement an effective scalable network**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-2

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- **EIGRP Overview**
- **EIGRP Operations**
- **EIGRP DUAL**
- **Configuring and Verifying EIGRP**
- **Advanced EIGRP Configuration Options**
- **EIGRP in a Scalable Network**
- **Lesson Assessments**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-3

EIGRP Overview

Overview

This lesson reviews the benefits of EIGRP and discusses the three databases that EIGRP uses in the path selection process. This lesson also defines common EIGRP terminology and provides a detailed look at the EIGRP metric calculation.

Relevance

To select the appropriate routing protocols for an internetwork, you must understand the key features and terminology that is necessary to evaluate a given protocol against other choices. Routing protocols are distinguished by the way that they select the best pathway and the way that they calculate the routing protocol metric.

Objectives

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

- Define the key features of EIGRP
- List the types of EIGRP databases
- Describe the EIGRP metrics calculation

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience
- Understanding of networking terms, numbering schemes, and topologies
- Understanding of the TCP/IP stack and how to configure IP addresses
- Ability to interpret the contents, entries, and indicators from a Cisco routing table

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Introduction**
- **EIGRP Databases**
- **EIGRP Metrics Calculation**
- **Summary**
- **Quiz**

Introduction

This topic describes EIGRP benefits and features and the topologies that EIGRP supports.

EIGRP Features

Cisco.com

The diagram illustrates an EIGRP network topology. At the top, a cloud labeled 'Core' contains four routers connected in a diamond shape. Router 10.1.0.0 is at the top-left, 10.2.0.0 is at the top-right, 10.3.0.0 is at the bottom-right, and 10.2.1.0 is at the bottom. Router 10.1.0.0 is connected to 10.1.1.0 and 10.1.4.0. Router 10.2.0.0 is connected to 10.2.1.0 and 10.3.1.0. Router 10.3.0.0 is connected to 10.3.1.0 and 10.3.2.0. Router 10.2.1.0 is connected to 10.2.2.0 and 10.2.3.0. Router 10.3.1.0 is connected to 10.3.2.0 and 10.3.3.0. Router 10.2.2.0 is connected to 10.2.3.0. Router 10.1.1.0 has an interface connected to subnet 10.1.1.0. Router 10.1.4.0 has interfaces connected to subnets 10.1.2.0 and 10.1.3.0. Router 10.3.2.0 has an interface connected to subnet 10.3.2.0. Router 10.3.3.0 has an interface connected to subnet 10.3.3.0. Router 10.2.3.0 has an interface connected to subnet 10.2.3.0. Router 10.2.2.0 has an interface connected to subnet 10.2.2.0.

- Advanced distance vector
- Rapid convergence
- 100% loop-free classless routing
- Easy configuration
- Incremental updates
- Load balancing across equal- and unequal-cost pathways
- Flexible network design
- Multicast and unicast instead of broadcast address
- Support for VLSM and discontiguous subnets
- Manual summarization at any point in the internetwork
- Support for multiple network-layer protocols

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 3-4

EIGRP is a Cisco proprietary protocol that combines the advantages of link-state and distance vector routing protocols. A hybrid protocol, EIGRP includes the following features:

- **Rapid convergence:** EIGRP uses DUAL to achieve rapid convergence. A router using EIGRP stores all available backup routes for destinations so that 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. EIGRP transmits these queries until it finds an alternate route.
- **Reduced bandwidth usage:** EIGRP does not make periodic updates. Instead, it sends partial updates when the path or the metric changes for that route. When path information changes, DUAL sends an update about only that link rather than the entire table. DUAL sends the information only to the routers that require it, in contrast to link-state protocols, in which an update is transmitted to all link-state routers within an area.
- **Multiple network-layer support:** EIGRP supports AppleTalk, IP, and Novell NetWare through the use of protocol-dependent modules (PDMs). PDMs are responsible for protocol requirements specific to the network layer.

Note This course covers only TCP/IP implementations of EIGRP.

- **Seamless connectivity across all data-link layer protocols and topologies:** EIGRP does not require special configuration to work across any Layer 2 protocols. Other routing protocols, such as Open Shortest Path First (OSPF), use different configuration for different Layer 2 protocols, such as Ethernet and Frame Relay. Commands that are unique to EIGRP can help limit the amount of bandwidth that EIGRP uses on WAN links.

EIGRP operates effectively in both LAN and WAN environments. WAN support for dedicated point-to-point links and nonbroadcast multiaccess (NBMA) topologies is standard for EIGRP. EIGRP accommodates differences in media types and speeds when neighbor adjacencies form across WAN links.

EIGRP has its roots as a distance vector routing protocol and is predictable in its behavior. Like its predecessor, Interior Gateway Routing Protocol (IGRP), EIGRP is easy to configure and is adaptable to a wide variety of network topologies. The addition of several link-state features, such as dynamic neighbor discovery, makes EIGRP an advanced distance vector protocol. EIGRP is an *enhanced* IGRP because of its rapid convergence and the guarantee of a loop-free topology at all times.

EIGRP is compatible with existing IGRP networks and, at the same time, offers clear advantages in the default behavior. IGRP performs periodic updates, which consumes bandwidth. IGRP performs triggered updates when there is a change in network topology. EIGRP performs only triggered routing updates, and the information exchanged between routers is limited to the affected routes only. Because EIGRP is a classless routing protocol, it advertises a routing mask for each destination network. The routing mask feature enables EIGRP to support discontiguous subnetworks and variable-length subnet masking (VLSM).

An additional feature that proves valuable for multiprotocol networks is support of Internetwork Packet Exchange (IPX) and AppleTalk. The rapid convergence and sophisticated metric structure of EIGRP offers superior performance and stability when implemented in IPX and AppleTalk networks.

EIGRP offers many advantages over traditional distance vector routing protocols. One of the most significant advantages exists in the area of bandwidth use. EIGRP uses multicast and unicast rather than broadcast. As a result, end stations are unaffected by routing updates and requests for topology information.

EIGRP uses the same algorithm for metric calculation as IGRP, but represents values in 32-bit format to give it additional granularity. EIGRP supports unequal metric load balancing, which allows administrators to better distribute traffic flow in their networks.

EIGRP borrows some of its operational characteristics from link-state protocols; for example, EIGRP allows administrators to create summary routes anywhere within the network, rather than rely on the traditional distance vector approach to perform classful route summarization at only major network boundaries. In addition, EIGRP supports bidirectional route redistribution from other routing domains at the process level.

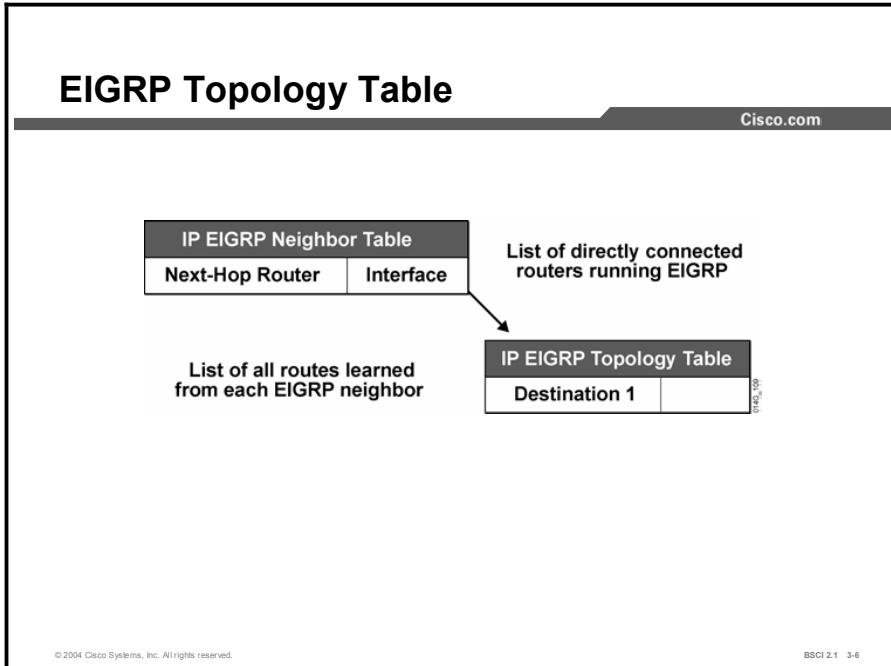
EIGRP Databases

This topic reviews the EIGRP neighbor and topology databases and their relationship to the IP routing table. This topic also defines key fields in the EIGRP topology table and explains their association with the IP routing table.

EIGRP Neighbor Table	
IP EIGRP Neighbor Table	
Next-Hop Router	Interface
List of directly connected routers running EIGRP 0140_308	

Each EIGRP router maintains a neighbor table. The table includes the following characteristics:

- Contains a list of directly connected EIGRP routers with an adjacency with this router
- Is comparable to the adjacencies database that link-state routing protocols uses and serves the same purpose: to ensure bidirectional communication between each of the directly connected neighbors
- Exists for each routed protocol that EIGRP supports

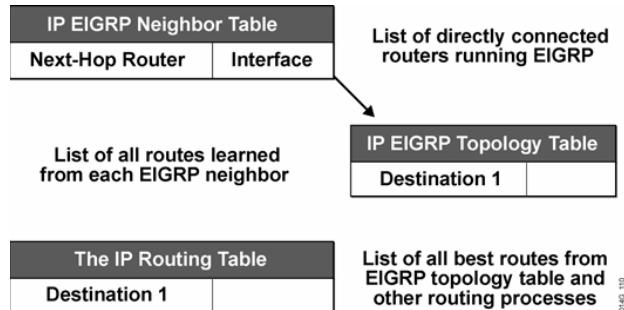


Each EIGRP router maintains a topology table for each routed protocol configuration. The topology table includes route entries for every destination that the router learns. The topology table maintains all learned routes to a destination with the following procedure:

1. Each neighbor in the EIGRP neighbor table forwards a copy of its IP routing table to all adjacent EIGRP neighbors.
2. Each neighbor then stores the routing table of the adjacent routers in the EIGRP topology database.
3. EIGRP examines the EIGRP topology database for all possible routers and selects the best route to every destination network.
4. 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 per routed protocol (IP, IPX, AppleTalk) configured.

EIGRP and IP Routing Table

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

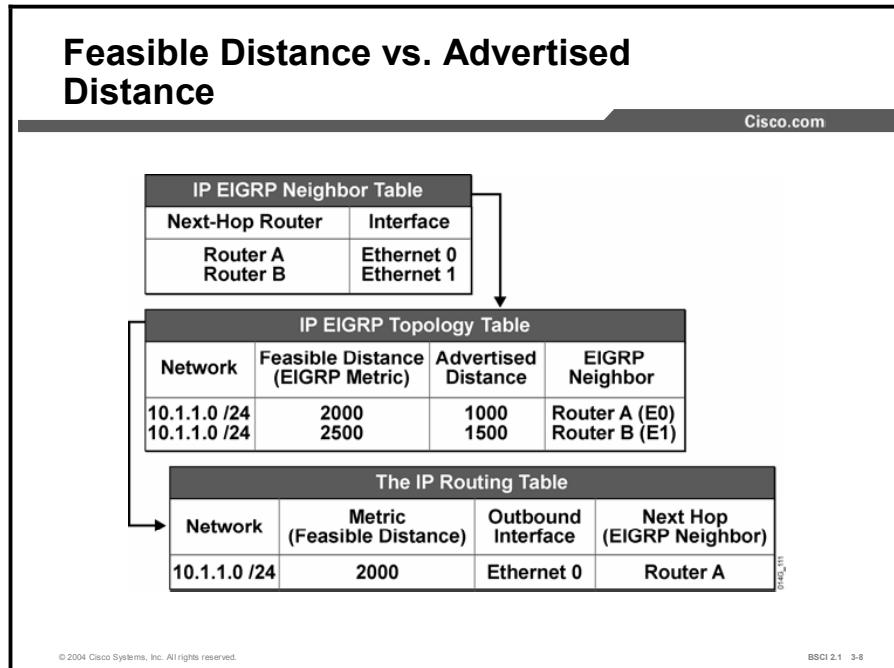
BSGI 2.1 3-7

To determine the successor (best route) and the feasible successor (backup route) to a destination, EIGRP uses the following two parameters:

- **Advertised distance:** The EIGRP metric for an EIGRP neighbor to reach a particular network
- **Feasible distance:** The advertised distance for a particular network learned from an EIGRP neighbor plus the EIGRP metric to reach that neighbor

The new total distance (metric) becomes the feasible distance. A router compares all feasible distances to reach a specific network and then selects the lowest feasible distance and places it in the IP routing table. The feasible distance for the chosen route becomes the EIGRP routing metric to reach that network in the routing table.

Example



The EIGRP topology database contains all the routes known to each EIGRP neighbor. As shown in the example, routers A and B sent their routing tables to router C, whose table is displayed in the figure. Both routers A and B have pathways to network 10.1.1.0/24, among many others that are not shown.

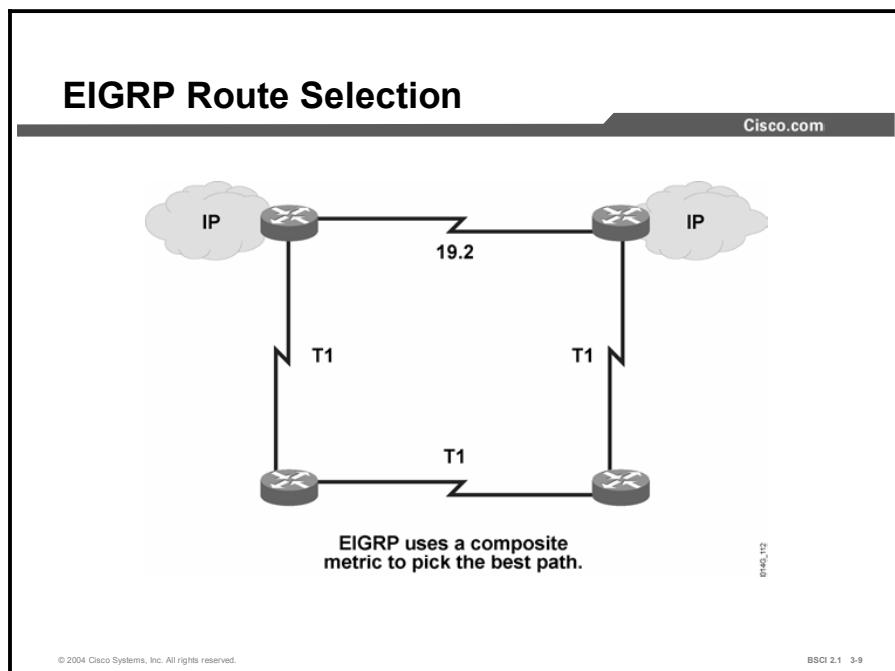
The routing table on router A shows an EIGRP metric of 1000. Router A advertises 10.1.1.0/24 to router C with a metric of 1000. Router C installs 10.1.1.0/24 from router A in its EIGRP topology table with an advertised distance of 1000. Router B has network 10.1.1.0/24 with a metric of 1500 in its IP routing table. Router B advertises 10.1.1.0/24 to router C with an advertised distance of 1500. Router C places the 10.1.1.0/24 network from router B in the EIGRP topology table with an advertised distance of 1500.

Router C has two entries to reach 10.1.1.0/24 in its topology table. The EIGRP metric for router C to reach both routers A and B is 1000. Add this cost (1000) into the respective advertised distance for each router, and the results represent the feasible distances that router C must travel to reach network 10.1.1.0/24.

Router C chooses the least-cost feasible distance (2000) and installs it in the IP routing table as the best route to reach 10.1.1.0/24. The EIGRP metric in the routing table equals the feasible distance from the EIGRP topology table.

EIGRP Metrics Calculation

This topic explains how to perform the EIGRP metrics calculation and how it is backward-compatible to IGRP.



EIGRP route selection is perhaps what most clearly distinguishes it from other routing protocols. Key EIGRP characteristics are as follows:

- EIGRP selects primary and backup routes and keeps them in the topology table (up to six per destination), and then places the primary routes in a routing table. EIGRP supports several route types: internal, external (non-EIGRP), and summary.
- EIGRP uses the same composite metric as IGRP to determine the best path, except that the EIGRP metric is multiplied by 256. The metric can be based on five criteria, but EIGRP uses only two of these criteria by default:
 - **Bandwidth:** The smallest bandwidth between source and destination
 - **Delay:** The cumulative interface delay along the path

The following criteria can be used, but are not recommended, because they typically result in frequent recalculation of the topology table:

- **Reliability:** This value represents the worst reliability between source and destination, based on keepalives.
- **Loading:** This value represents the worst load on a link between source and destination, computed based on the packet rate and the configured bandwidth of the interface.
- **Maximum transmission unit (MTU):** This criterion represents the smallest MTU in path. MTU is included in the EIGRP routing update but is not actually used in the metric calculation.

EIGRP uses DUAL to calculate the best route (successor route) to a destination. DUAL selects routes based on the composite metric and ensures that the selected routes are loop-free. DUAL also calculates a backup route (feasible successor route) to a destination that is loop-free. If the best route fails, EIGRP immediately uses the backup route without any need of holddown, because the backup route is loop-free, which results in fast convergence.

EIGRP Metrics Calculations

Cisco.com

- When the K constants are set to default settings (recommended):

$$\text{Metric} = [K1 * BW + ((K2 * BW) / (256 - \text{load})) + K3 * \text{delay}]$$

- By default: $K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0$

- By default, EIGRP metric = BW [lowest link] + delay [sum of links].

- BW = the lowest link-bandwidth along the path

- When K5 is changed to a value of 1 (not recommended):

$$\text{Metric} = [K1 * BW + ((K2 * BW) / (256 - \text{load})) + K3 * \text{delay}] * [K5 / (\text{reliability} + K4)]$$

$$* [K5 / (\text{reliability} + K4)]:$$

- $K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 1$

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-10

If K5 is not equal to zero, EIGRP uses the following formula to calculate a metric:

- Metric = $[K1 * \text{bandwidth} + (K2 * \text{bandwidth}) / (256 - \text{load}) + K3 * \text{delay}] * [K5 / (\text{reliability} + K4)]$

If K5 is equal to zero, then the metric formula is:

- $[K1 * \text{bandwidth} + (K2 * \text{bandwidth}) / (256 - \text{load}) + K3 * \text{delay}]$

Then, if $K1 = 1, K2 = 0$, and $K3 = 1$:

- Metric = bandwidth + delay

Modification of the K values permits the administrator to factor delay and reliability into the EIGRP metric. Note that modification of these values is generally not recommended.

EIGRP hello packets carry the K values. EIGRP does not form a neighbor relationship if the K values do not match between the routers. Metric compilation by default uses only K1 and K3 values, which you should modify only after extremely careful planning. A change to these values can cause your network to fail to converge.

The formats of the delay and bandwidth values used for EIGRP metric calculations are different from those displayed using the **show interface** command. The EIGRP delay value is the sum of the delays in the path, in tens of microseconds, multiplied by 256. Note that the **show interface** command displays delay in microseconds. Calculate the EIGRP bandwidth using the minimum bandwidth link along the path, in kilobits per second. Divide 10^7 by this value, and then multiply the result by 256.

EIGRP Metrics Backward-Compatible to IGRP

Cisco.com



172.16.0.0 IGRP metric 1000 → 172.16.0.0 EIGRP metric 256000

192.168.6.0 IGRP metric 2000 ← 192.168.5.0 EIGRP metric 512000

IGRP metric = EIGRP metric / 256 EIGRP metric = IGRP metric × 256
IGRP metric is 24 bits in length EIGRP metric is 32 bits in length

256 = 8 bits

DIA02_14

©2004 Cisco Systems, Inc. All rights reserved.

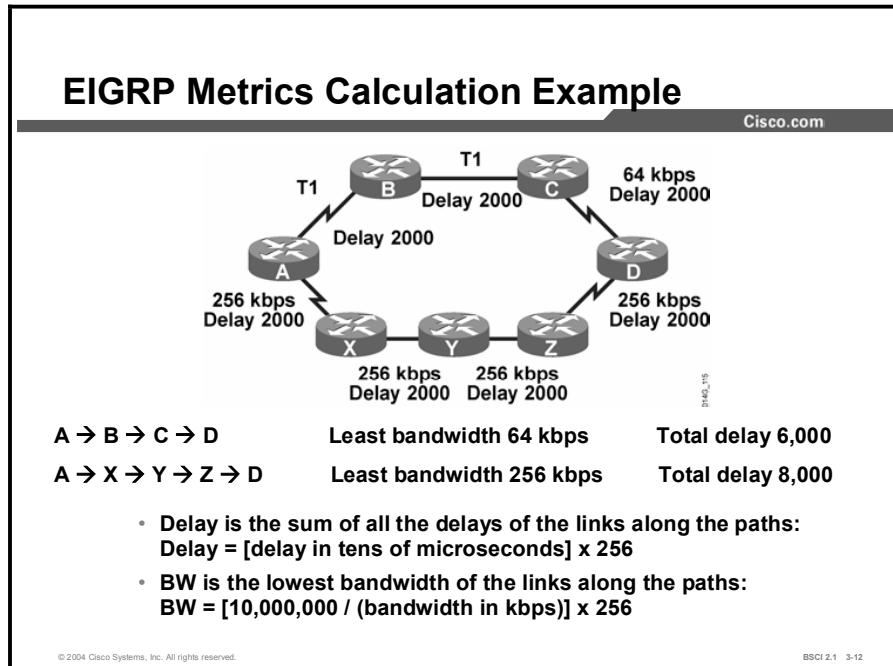
BSCI 2.1 - 3-11

EIGRP represents its metrics in a 32-bit format, versus the 24-bit representation used by IGRP. The 32-bit representation allows for a more granular decision to calculate the best routes.

Note that present-day bandwidth ranges from 9600 to 9,984,000,000 bits per second (almost 10 Gb). The EIGRP 32-bit metric accommodates this range better than the IGRP 24-bit number.

The EIGRP metric value ranges from 1 to 4,294,967,296. The IGRP metric value ranges from 1 to 16,777,216. When integrating IGRP routes into an EIGRP domain using redistribution, the router multiplies the IGRP metric by 256 to compute the EIGRP-equivalent metric. When sending EIGRP routes to an IGRP routing domain, the router divides each EIGRP metric by 256 to achieve the proper 24-bit metric.

Example



In the figure, router A has two pathways to reach networks behind router D.

The bandwidth through the top pathway ($A \rightarrow B \rightarrow C \rightarrow D$) is as follows:

- AB—T1, BC—T1, and CD—64 kbps

The least bandwidth along this path is 64 kbps:

$$\text{■ } 10,000,000 / 64 = 156,250 * 256 = 40,000,000$$

In this example, the delay through the top pathway is as follows:

- EIGRP delay calculation for a T1 (1.544 megabits) has an EIGRP delay of 2000 (in tens of milliseconds) * 256 = 512,000
- EIGRP delay calculation for a 64,000-bps line has an EIGRP delay of 2000 (in tens of milliseconds) * 256 = 512,000
- 512,000 (AB) + 512,000 (BC) + 512,000 (CD) = total delay of 1,536,000
- Bandwidth (40,000,000) plus delay (1,536,000) = EIGRP metric of 41,536,000 for the top pathway

The bandwidth through the bottom pathway ($A \rightarrow X \rightarrow Y \rightarrow Z \rightarrow D$) is as follows:

- AX—256 kbps, XY—256 kbps, YZ—256 kbps, and ZD—256 kbps

The least bandwidth along this path is 256 kbps:

$$\text{■ } 10,000,000 / 256 = 39,062 * 256 = 10,000,000$$

The delay through the bottom pathway is as follows:

- EIGRP delay calculation for a 256,000-bps line has an EIGRP delay of 2000 (in tens of milliseconds) * 256 = 512,000
- 512,000 (AX) + 512,000 (XY) + 512,000 (YZ) + 512,000 (ZD) = total delay of 2,048,000
- Bandwidth (10,000,000) plus delay (2,048,000) = EIGRP metric of 12,048,000 for the bottom pathway

EIGRP chooses the bottom pathway, with a metric of 12,048,000, over the top pathway, with a metric of 41,536,000. EIGRP then installs the bottom pathway with a next-hop router of X and a metric of 12,048,000 in the IP routing table.

Why is the bottom pathway considered a better pathway?

The bottleneck along the top pathway, the 64,000-bps link, can explain why the router takes this path. The link means that the rate of transfer to router D is a maximum of 64,000 bps. Along the bottom pathway, the lowest speed is 256,000 bps, making the throughput rate up to that speed. Therefore, the bottom pathway represents a better choice to move large files quickly.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **EIGRP is a 100% loop-free advanced distance vector routing protocol that is easy to configure and has many advanced features, such as classless routing, VLSM, and incremental updates.**
- **EIGRP uses three databases:**
 - EIGRP neighbor database
 - EIGRP topology database
 - IP routing table
- **EIGRP uses the same basic algorithm for metric calculation as IGRP, which allows EIGRP to be backward-compatible to IGRP. For both protocols, the default calculation relies on bandwidth and delay.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-13

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 features are benefits of EIGRP? (Choose three.)
- A) fast convergence
 - B) support for VLSM and discontiguous subnets
 - C) same metric algorithm as OSPF
 - D) manual route summarization at any point in the network
- Q2) What is listed in the EIGRP topology database?
- A) directly connected routers that have formed an EIGRP adjacency
 - B) only best routes to a destination network
 - C) all routes learned from each EIGRP neighbor
- Q3) What is listed in the EIGRP neighbor database lists?
- A) directly connected routers that have formed an EIGRP adjacency
 - B) only best routes to a destination network
 - C) all routes learned from each EIGRP neighbor
- Q4) What is listed in the IP routing table lists?
- A) directly connected routers that have formed an EIGRP adjacency
 - B) only best routes to a destination network
 - C) all routes learned from each EIGRP neighbor
- Q5) Which two of the following are true of the EIGRP metric calculation? (Choose two.)
- A) The following are the default K values: K1 = 1, K2 = 1, K3 = 0, K4 = 0, K5 = 0.
 - B) To convert an IGRP metric to an EIGRP metric, multiply the IGRP metric by 256.
 - C) To convert an IGRP metric to an EIGRP metric, multiply the EIGRP metric by 256.
 - D) The following are the default K values: K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0.

Quiz Answer Key

Q1) A, B, D

Relates to: EIGRP Overview

Q2) C

Relates to: EIGRP Databases

Q3) A

Relates to: EIGRP Databases

Q4) B

Relates to: EIGRP Databases

Q5) B, D

Relates to: EIGRP Metrics Calculation

EIGRP Operations

Overview

This lesson examines the five EIGRP packets and describes the initial establishment of adjacency between EIGRP neighbors. The hello packet that builds these adjacencies and the key fields in the hello packet are explained. The mechanisms for reliability, transmission, and resetting EIGRP adjacencies are defined and explained. Finally this lesson demonstrates the Cisco IOS **debug** and **show** commands used for troubleshooting these adjacencies.

Relevance

It is important for network administrators to understand the exchange of EIGRP packets and the functions of EIGRP packets to troubleshoot an EIGRP network. If EIGRP does not form neighbor relationships, those routers do not exchange EIGRP updates with each other. Without EIGRP routing updates, users cannot connect to services across the internetwork. This lesson explains which hello fields are necessary for adjacency to form and when it resets; this information is vital for troubleshooting an EIGRP network.

Objectives

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

- Describe EIGRP packets
- Explain EIGRP adjacent neighbors
- Define EIGRP reliability, transmission policy, and transport mechanism
- Describe initial route discovery
- Interpret debug output for EIGRP packets, EIGRP neighbors, and IP EIGRP

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- Knowledge of the Cisco router user interface
- Understanding of how to read an IP routing table
- Understanding of networking terms, numbering schemes, and topologies
- Understanding of how to interpret the contents, entries, and indicators from a Cisco routing table
- Understanding of how to verify basic router configurations using **show** and **debug** command output

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **EIGRP Packets**
- **Establishing Neighbors**
- **EIGRP Reliability, Transmission Policy, and Transport Mechanism**
- **Initial Route Discovery in EIGRP**
- **Verifying EIGRP Connectivity Using debug Commands**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-3

EIGRP Packets

This topic identifies the five EIGRP packet types. This topic also details the EIGRP hello packet and explains the role that the hello packet plays in maintaining connectivity between EIGRP neighbors.

EIGRP Packets

Cisco.com

- **Hello:** Establish neighbor relationships
- **Update:** Send routing updates
- **Query:** Ask neighbors about routing information
- **Reply:** Respond to query about routing information
- **ACK:** Acknowledge a reliable packet

© 2004 Cisco Systems, Inc. All rights reserved.

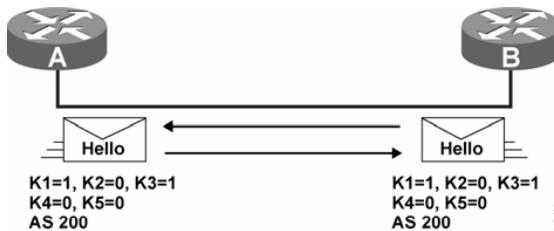
BSCI 2.1 3-4

EIGRP supports the following five generic packet types:

- **Hello:** Routers use hello packets for neighbor discovery. They send the packets as multicasts, and the packets carry an acknowledgment number of zero.
- **Update:** Update packets route reliable change information only to the affected routers. These updates can be unicast to a specific router or multicast to multiple attached routers. Updates occur during router startup, metric or topology change, and route transition from active to passive.
- **Query:** When a router performs route computation and does not have a feasible successor, it sends a reliable query packet to its neighbors to determine if they have a feasible successor for the destination. Queries are always multicast.
- **Reply:** A router sends a reply packet in response to a query packet. Replies are unicast reliably to the originator of the query.
- **Acknowledgment (ACK):** The ACK packet acknowledges the types of packets described in this topic. ACK packets are unicast hello packets and contain a nonzero acknowledgment number. Update, query, and reply packets are all sent reliably. These packets require acknowledgment, in contrast to hello and ACK packets, which do not.

EIGRP Hello Packets

Cisco.com



- Two routers become neighbors when they see the hello packet of the other router.
 - Hello address = 224.0.0.10
- EIGRP does not form neighbors if K values are mismatched.
- EIGRP does not form neighbors if autonomous system numbers are mismatched.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

When you configure EIGRP on an interface, the router sends periodic multicast hello packets out that interface. When a router running an EIGRP process receives a hello packet from another router with the same autonomous system number, it establishes a neighbor relationship (adjacency).

Peer relationships do not form if the neighbor resides in a different autonomous system or if the metric-calculation mechanism (K value) is mismatched.

EIGRP Hello Timers

Cisco.com

- **Hello sent once every 5 seconds on the following links:**
 - Broadcast media: Ethernet, Token Ring, FDDI
 - Point-to-point serial links: PPP, HDLC
 - Point-to-point subinterface: Frame Relay, ATM
 - Multipoint circuits with bandwidth greater than T1: SMDS, Frame Relay, ATM, ISDN PRI
- **Hello sent once every 60 seconds on the following links:**
 - Multipoint circuits with bandwidth less than or equal to T1: ISDN BRI, Frame Relay, SMDS, ATM, and X.25
- **Hold time by default is three times the hello time.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 3-6

Hello packets are sent at various time intervals, depending on the media. The default is every 5 seconds over LAN and dedicated or higher-speed WAN links. (These links include, for broadcast media, Ethernet, Token Ring, and FDDI; for point-to-point serial links, PPP and HDLC; for point-to-point subinterfaces, Frame Relay and ATM; and for multipoint circuits with bandwidth greater than T1, Switched Multimegabit Data Service [SMDS], Frame Relay, ATM, and ISDN PRI.)

When you configure a router for EIGRP, the EIGRP process dynamically discovers other routers directly connected to it that run EIGRP. Each router maintains information about its neighboring routers in its neighbor table, including the address and the interface through which it reaches the neighbor. The neighbor table also maintains an entry for hold time, which a router reports as part of its hello message. Hold time is the interval that a router waits before it declares an EIGRP neighbor as unavailable.

EIGRP sends hello packets less frequently on lower-speed links. For example, multipoint serial interfaces of T1 or slower generate hellos at 60-second intervals on this type of interface. The hello interval is the rate at which hello packets are sent; this rate can be adjusted per interface with the **ip hello-interval eigrp** command, as follows:

```
RouterA(config-if)# ip hello-interval eigrp as-number seconds
```

If the router does not receive an EIGRP packet within the hold time interval, the neighbor and all routes associated with that neighbor are removed from the EIGRP databases. If the neighbor is a successor for any destination networks, those networks are removed from the routing table, and alternate pathways, if available, are computed. By default, the hold time is set to three times the hello interval. The hold time default values are 15 seconds and 180 seconds. The hold time can be adjusted with the **ip hold-time eigrp** interface command, as follows:

```
RouterA(config-if)# ip hold-time eigrp as-number seconds
```

Note	Hold time is not automatically adjusted after a hello interval change. Hold time must be adjusted manually to reflect the configured hello interval.
-------------	--

Establishing Neighbors

This topic discusses an EIGRP neighbor relationship establishment and the conditions for resetting an EIGRP adjacency.

EIGRP Adjacency Establishment Conditions

Cisco.com

The diagram shows two routers, A and B, connected by a horizontal line representing a link. Router A is on the left and router B is on the right. Each router has a small envelope icon below it, labeled "Hello", indicating the transmission of a hello packet. Router A's envelope is pointing towards router B, and router B's envelope is pointing towards router A, representing a bidirectional exchange of hello packets.

Source	Destination
10.1.1.1	224.0.0.10

Destination	Source
224.0.0.10	10.1.1.2

- **EIGRP does form neighbors even if hell time and hold time do not match.**
- **EIGRP transmits hello packets from the primary address of the interface.**
- **The neighbor declared dead when no EIGRP packets are received within the hold interval.**

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 3-7

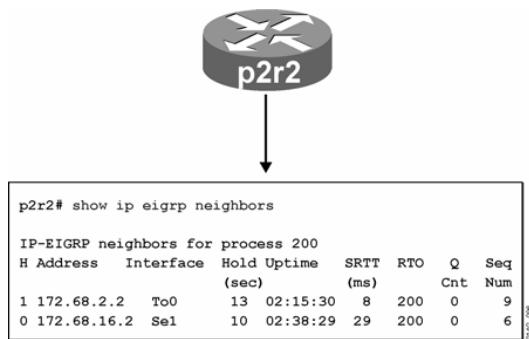
It is possible for two routers to become EIGRP neighbors even if the hello and hold times do not match. The hello packets include the hold time, and each router keeps track of the hold time associated with each EIGRP neighbor.

If an EIGRP packet is not received from a neighbor by a router that runs the EIGRP process before the expiration of the hold time, the router detects a topology change. The router deletes the neighbor adjacency, and all topology table entries recognized from that neighbor are removed. It is as if the neighbor sent an update that states that all of the routes were unreachable; this condition causes routes to enter an active state. This procedure enables the routes to reconverge quickly if an alternate, feasible route is available.

EIGRP does not build peer relationships over secondary addresses because all EIGRP traffic uses the primary address of the interface. To form an EIGRP adjacency, all neighbors use their primary address as the source IP address of their EIGRP packets. Adjacency between EIGRP routers takes place if the primary address of each neighbor is part of the same IP subnet.

show ip eigrp neighbors Command

Cisco.com



```
p2r2# show ip eigrp neighbors

IP-EIGRP neighbors for process 200
  H Address      Interface   Hold Uptime    SRTT     RTO      Q      Seq
               (sec)          (ms)          Cnt  Num
  1 172.68.2.2  To0          13  02:15:30    8  200      0      9
  0 172.68.16.2 Sel          10  02:38:29   29  200      0      6

```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

EIGRP routers multicast hello packets to discover neighboring routers and to exchange route updates. Recall that only adjacent routers exchange routing information. Each router builds a neighbor table from the hello packets it receives from adjacent EIGRP routers that run the same network-layer protocol.

EIGRP maintains a neighbor table for each configured network-layer protocol. The table includes the following key elements:

- **Neighbor address:** Specifies the network-layer address of the neighbor.
- **Queue:** Indicates the number of packets waiting in the queue to be sent. If this value is constantly higher than zero, there can be a congestion problem. A zero indicates that there are no EIGRP packets in the queue.
- **Smoothed round trip time (SRTT):** Indicates the average time it takes to send and receive packets from a neighbor. This timer is used to determine the retransmission timeout (RTO).
- **RTO:** The time, in milliseconds, that the router waits for an acknowledgment before it retransmits the reliable packet.
- **Hold time:** The maximum time to wait without having received anything from a neighbor before considering the neighbor unavailable. Originally, the expected packet was a hello packet, but in current Cisco IOS software releases, any EIGRP packet the router receives after the first hello packet resets the timer.

EIGRP Reliability, Transmission Policy, and Transport Mechanism

This topic discusses the operations involved in maintaining the EIGRP databases and neighbor relationships.

EIGRP Reliability

Cisco.com

- **EIGRP reliable packets are packets that require explicit acknowledgment:**
 - Update
 - Query
 - Reply
- **EIGRP unreliable packets are packets that do not require explicit acknowledgment:**
 - Hello
 - ACK

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-9

The Rapid Transport Protocol (RTP) is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. RTP supports intermixed transmission of multicast or unicast packets. For efficiency, only certain EIGRP packets transmit reliably. For instance, on a multiaccess network with multicast capabilities, such as an Ethernet network, it is not necessary to send hello packets reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello packet containing an indicator that informs the receivers that they do not need to acknowledge the packet.

Other types of packets, such as updates, indicate in the packet that EIGRP requires acknowledgment. All packets that carry routing information (update, query, and reply) are sent reliably because they are not sent periodically. Each packet that is sent reliably has an assigned sequence number and requires an explicit acknowledgement. This combination of sequence numbers and acknowledgements provides reliability. ACK and hello packets, by their nature, are not reliable transmissions.

RTP contains a provision to send multicast packets quickly when there are unacknowledged packets outstanding, which helps ensure fast convergence time over differing speed links.

EIGRP Retransmission Policy

Cisco.com

- The router keeps a neighbor list and a retransmission list for every neighbor.
- Each reliable packet (update, query, reply) is retransmitted when the packet is not acknowledged.
- A neighbor relationship is reset when the retry limit (16) for reliable packets is reached.
- Retransmission occurs each time the RTO is reached.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-10

RTP ensures that the router maintains ongoing communication between neighboring routers, and RTP maintains a retransmission list for each neighbor in case a reliable packet is not acknowledged within the RTO. This list is used to track all the reliable packets that were sent out but not acknowledged. The RTO sometimes expires before it receives an ACK packet. In this event, the EIGRP process retransmits another copy of the reliable packet, up to a maximum of 16 times or until the hold time expires.

The EIGRP reliability mechanism ensures delivery of critical route information to neighboring routers. This information allows EIGRP to maintain a loop-free topology at all times.

EIGRP Transport Mechanism

Cisco.com

- **EIGRP transport has a window size of one (stop-and-wait mechanism).**
 - **Each reliable packet needs to be acknowledged before the next sequenced packet can be sent.**
 - **If one or more peers are slow in acknowledging, all other peers suffer.**
- **Solution: The nonacknowledged multicast packet is retransmitted as a unicast to the slow neighbor.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-11

The use of reliable multicast traffic by IP routing protocols is efficient and effective, although a potential delay exists on multiaccess media where multiple neighbors exist. The next reliable multicast packet cannot be transmitted until all peers have acknowledged the previous multicast. If one or more peers respond slowly, the slow EIGRP peer adversely affects all peers by delaying the next transmission. The RTP used by EIGRP has a provision for handling such situations. Neighbors that are slow to respond to multicasts receive the unacknowledged multicast packets again, this time as unicast packets. This design allows the reliable multicast operation to proceed without communication delays with other peers.

The multicast flow timer determines how long to wait for an ACK packet before switching from multicast to unicast. The RTO determines how long to wait between the subsequent unicasts. The EIGRP process for each neighbor based on the SRTT calculates both multicast flow timer and RTO. The formulas for the SRTT, RTO, and multicast flow timer are proprietary.

Example

Resetting of EIGRP Neighbors

Cisco.com

- **Stable network: no outstanding EIGRP updates**
 - Neighbor is reset if hold timer expires. Timer default is three times the hello interval:
 - 180 seconds on T1 or slower multipoint interfaces
 - 15 seconds on all others
- **Unstable network: reliable packet transfer in progress**
 - Neighbor is reset if update is not acknowledged after 16 retransmissions
 - Update retransmitted each time RTO is reached

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-12

In a steady-state network where no routes are flapping, EIGRP waits a specified interval before it determines that an EIGRP neighbor adjacency is down. By default, EIGRP waits up to 15 seconds on high-speed links and up to 180 seconds on low-speed, multipoint links. When EIGRP determines that a neighbor is down and the router cannot re-establish the adjacency, the routing table removes all networks that were reachable through that neighbor. The router attempts to find alternate routes to those networks so that convergence can occur.

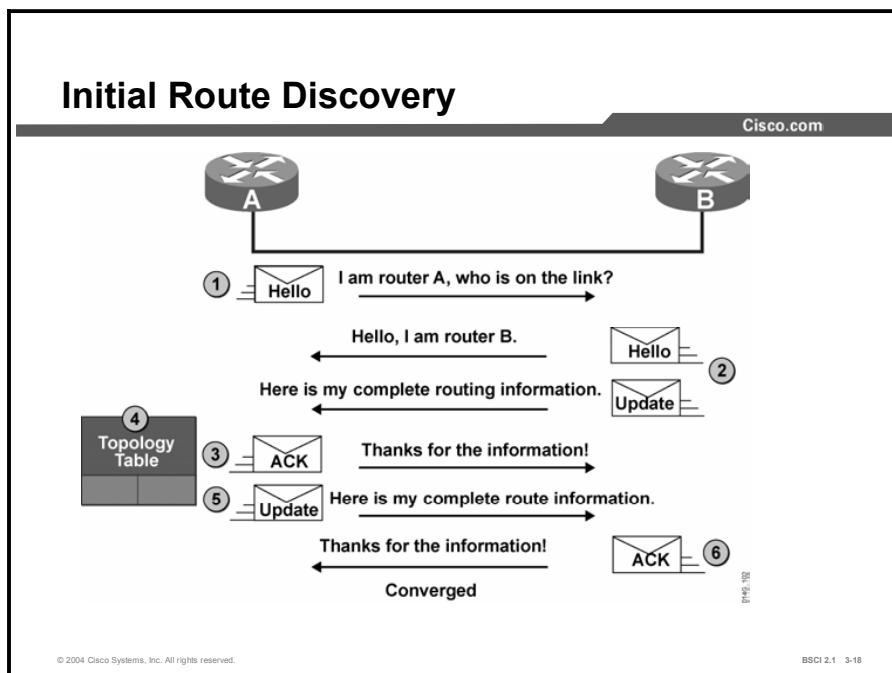
The 180-second hold time can seem excessive, but this duration accommodates the slowest-speed multipoint links, which are generally connected to less critical remote sites. In some networks with mission-critical, time-sensitive applications, even on high-speed links, 15 seconds is too long. The point to remember is that there are other conditions that can override the hold timer and allow the network to converge quickly.

If the network is unstable and routes are flapping elsewhere because a remote site is timing out on its adjacency, EIGRP hold timers begin counting down from 180 seconds. If the upstream site sends the remote site an update and the remote site does not acknowledge the update, the upstream site attempts 16 times to retransmit the update. The retransmission occurs each time the RTO expires. After 16 retries, the router resets the neighbor relationship. This causes the network to converge faster than would be possible by waiting for the hold time to expire.

RTO is a dynamic timer that adjusts over time. It is based upon the SRTT, which specifies how many milliseconds it takes a neighbor to respond to an EIGRP acknowledgment. As more unacknowledged updates are sent, the SRTT gets higher and higher, which causes the RTO to increase exponentially.

Initial Route Discovery in EIGRP

This topic shows the exchange of packets for the initial exchange of routing information between new EIGRP neighbors.



The process to establish and discover neighbor routes occurs simultaneously in EIGRP. A high-level description of the process is as follows:

- Step 1** A new router (router A) comes up on the link and sends a hello packet from all interfaces.
- Step 2** Routers that receive the hello packet (router B) reply with update packets that contain all the routes in their routing tables, except those that the interface recognizes through that interface (split horizon). Router B sends an update packet to router A, but a neighbor relationship is not established until router B sends a hello packet to router A. The update packet from router B has the initialization bit set, indicating that this is the initialization process.

Note	An update packet includes information about the routes that a neighbor is aware of, including the metric that the neighbor is advertising for each destination.
-------------	---

- Step 3** After both routers have exchanged hellos, and the neighbor adjacency is established, router A replies to router B with an ACK packet that indicates that it has received the update information.
- Step 4** Router A assimilates all update packets in its topology table. The topology table includes all destinations advertised by neighboring (adjacent) routers. It lists each destination, all the neighbors that can reach the destination, and their associated metric.

Step 5 Router A then sends an update packet to router B.

Step 6 Upon receiving the update packet, router B sends an ACK packet to router A.

After router A and router B successfully receive the update packet from each other, they are ready to update the routing table with the successor routes from the topology table.

Verifying EIGRP Connectivity Using debug Commands

This topic describes the output of EIGRP **debug** commands, such as **debug eigrp packets** and **debug ip eigrp**.

Verifying EIGRP Connectivity: Stable Network

Cisco.com

```
RouterA# debug eigrp packets

      Normal Hello Processing
01:38:29: EIGRP: Sending HELLO on Serial0/0
01:38:29: AS 100, Flags 0x0, Seq 0/0 iidbQ 0/0 iidbQ un/rely 0/0
01:38:31: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:38:31: AS 100, Flags 0x0, Seq 0/0 iidbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
      Received EIGRP Update
01:38:33: EIGRP: Received UPDATE on Serial0/0 nbr 10.1.2.2
01:38:33: AS 100, Flags 0x0, Seq 23/37 iidbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:38:33: EIGRP: Enqueueing ACK on Serial0/0 nbr 10.1.2.2
01:38:33: Ack seq 23 iidbQ un/rely 0/0 peerQ un/rely 1/0
01:38:33: EIGRP: Sending ACK on Serial0/0 nbr 10.1.2.2
01:38:33: AS 100, Flags 0x0, Seq 0/23 iidbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 1/0
01:38:33: EIGRP: Enqueueing UPDATE on Serial0/0 iidbQ un/rely 0/1 serno 75-75
01:38:33: EIGRP: Sending UPDATE on Serial0/0 nbr 10.1.2.2
01:38:33: AS 100, Flags 0x0, Seq 38/23 iidbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
      serno 75-75
01:38:33: EIGRP: Received ACK on Serial0/0 nbr 10.1.2.2
01:38:33: AS 100, Flags 0x0, Seq 0/38 iidbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
```

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 3-19

This **debug** command can be used to verify EIGRP connectivity.

Command	Description
debug eigrp packets	Displays the types of EIGRP packets sent and received by the router that this command is executed on. A maximum of 11 packet types can be selected for individual or group display.

Note Use extreme care when using debugs in production networks. The resources used for the debug can be significant and reduce processing of user traffic.

The **debug eigrp packet** command traces transmission and receipt of EIGRP packets. The **debug** output shows normal transmission and receipt of hello packets. The serial link is a High-Level Data Link Control (HDLC) point-to-point link; therefore, the default hello time interval is 5 seconds. Hello packets are unreliable sent, so the sequence number (Seq) does not increment.

When router A in this example output receives an update from the 10.1.2.2 neighbor, values appear in the sequence number field. The Seq 23/37 field indicates that 10.1.2.2 is sending this packet as sequence number 23 to router A and that sequence number 37 has been received from router A by neighbor 10.1.2.2. Neighbor 10.1.2.2 is expecting to receive sequence 38 in the next reliable packet from router A.

The serial number (serno 75/75) reflects the number of changes that the two neighbors register in their EIGRP topology tables. The sequence number increments each time a query, update, or reply packet is sent, whereas the serial number increments each time the topology table changes. A single update can contain more than 100 networks that all produce an update because all are now unavailable. Therefore, in this case, the topology table has more than 100 changes, and the serial number increases substantially but the sequence number increases only by one.

Verifying EIGRP Connectivity: Unstable Network

Cisco.com

```
RouterA# debug eigrp packets

      Shut down of a neighbor's interface
01:38:11: EIGRP: Received QUERY on Serial0/0 nbr 10.1.2.2
01:38:11:   AS 100, Flags 0x0, Seq 22/36 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
01:38:11: EIGRP: Enqueuing ACK on Serial0/0 nbr 10.1.2.2
01:38:11:   Ack seq 22 iidbQ un/rely 0/0 peerQ un/rely 1/0
01:38:11: EIGRP: Sending ACK on Serial0/0 nbr 10.1.2.2
01:38:11:   AS 100, Flags 0x0, Seq 0/22 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 1/0
01:38:11: EIGRP: Sending REPLY on Serial0/0 nbr 10.1.2.2
01:38:11:   AS 100, Flags 0x0, Seq 37/22 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 74-74
01:38:11: EIGRP: Received ACK on Serial0/0 nbr 10.1.2.2
01:38:11: AS 100, Flags 0x0, Seq 0/37 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
```

```
RouterA# debug eigrp packets

Mismatched adjacency values
01:39:13: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:39:13:   K-value mismatch
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-20

In this example, an interface on router B (EIGRP neighbor 10.1.2.2) is shut down. Router B then sends a query packet to router A to determine if router A knows a pathway to the lost network. Router A responds with an ACK packet to acknowledge the query packet. A reliable packet must be explicitly acknowledged with an ACK packet. Router A also responds to the query with a reply packet. The serial number reference (74) represents the number of changes to the routing table since the start of the neighbor relationship between these two EIGRP neighbors.

The debug output list at the bottom of the figure indicates that the router received a hello packet from neighbor 10.1.2.2 with mismatched K values. The neighbor configuration is K1 = 1, K2 = 1, K3 = 1, K4 = 1, and K5 = 1. The router configuration is default K values, so an adjacency between these two neighbors is not formed until the K values are equal.

Verifying EIGRP Operations: Stable Network

Cisco.com

```
RouterA# debug ip eigrp
IP-EIGRP Route Events debugging is on
01:57:23: IP-EIGRP: Processing incoming UPDATE packet
01:57:23: IP-EIGRP: Int 172.16.1.0/24 M 10639872 - 9999872 640000
SM 384000 - 256000 128000
```

- Router A receives an update packet from router B that contains internal (int) network 172.16.1.0/24.
- Feasible distance = router A cost to get to 172.16.1.0/24.
 $10639872 = 9999872 + 640000$
- Advertised distance = the metric router B sent to router A to reach 172.16.1.0/24.
 $SM \text{ (source metric)} = 384000 = 256000 + 128000$
- EIGRP metric (10639872) = bandwidth (9999872) + delay (640000).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-21

This **debug** command can be used to verify EIGRP operation.

Command	Description
debug ip eigrp	Displays EIGRP packets that this router sends and receives

This figure illustrates the contents of the updates that are reported when you use the **debug ip eigrp** command to monitor a stable network.

An internal route (Int) for 172.16.1.0/24 is advertised to router A. Its feasible distance is the EIGRP metric calculation for lowest bandwidth plus the EIGRP metric calculation for the total delay.

The following is an example of the EIGRP metric calculation for the total delay:

- M 10639872 – 9999872 640000, which stands for metric = $10639872 = 9999872 + 640000$

The EIGRP process uses the following information to calculate the advertised distance and place it in the EIGRP topology table:

- SM 384000 – 256000 128000, which means source metric = $384000 = 256000 + 128000$

Verifying EIGRP Operations: Unstable Network

Cisco.com

```
RouterA# debug ip eigrp
```

IP-EIGRP Route Events debugging is on

- An EIGRP neighbor interface is shutdown for network 172.16.1.1/24.
- Router A receives a query looking for a lost pathway from Router B.

```
01:56:57: IP-EIGRP: Processing incoming QUERY packet
```

```
01:56:57: IP-EIGRP: Int 172.16.1.0/24 M 4294967295 - 0 4294967295 SM  
4294967295 - 0 4294967295
```

- The metric of 4,294,967,295 is the highest possible value for a metric. It signifies that router B is telling router A that network 172.16.1.0/24 is no longer reachable through router B, and router B checks whether router A has an alternate pathway to that network.

```
01:56:57: IP-EIGRP: 172.16.1.0/24 routing table not updated
```

```
01:56:57: IP-EIGRP: 172.16.1.0/24 - not in IP routing table
```

- Router A realizes that if it cannot use B for 172.16.1.0/24, it does not have an entry in the routing table to get to that network.

```
01:56:57: IP-EIGRP: Int 172.16.1.0/24 metric 4294967295 - 9999872  
4294967295
```

- Router A sends an update to router B saying it does not know how to reach that route either.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-22

This example illustrates what occurs when a router processes an incoming query packet for network 172.16.1.0/24. On the neighbor, the interface that leads to that network is shut down. The neighbor previously advertised 172.16.1.0 /24 to this router, and the query performs two functions:

- First, this router discovers that its neighbor no longer knows how to get to network 172.16.1.0 /24. This metric value (4,294,967,295) is the highest possible value. This metric indicates that the route is unreachable, so the router removes this entry from the EIGRP topology table, and EIGRP looks for alternate routes.
- If the routing table is not updated, EIGRP did not find an alternate route to the network. The next statement verifies that the EIGRP process has removed the old route. The final statement confirms that this router informed the neighbor that it does not have a pathway to this network either.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **EIGRP has five packet types:**
 - Update, query, and reply packets require acknowledgment.
 - Hello and ACK packets do not require acknowledgment.
- **EIGRP hello packets are used to build EIGRP adjacencies.**
- **By default, hellos are sent at the following intervals:**
 - Every 60 seconds on T1 or slower multipoint interfaces
 - Every 5 seconds on all others
- **The router resets the neighbor relationship when it reaches the retry limit (limit = 16) or when the hold time expires.**
- **Neighboring routers that are slow to respond to multicasts receive unacknowledged packets again as unicast packets.**

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 packet type establishes neighbor relationships?

- A) ACK
- B) hello
- C) query
- D) reply
- E) update

Q2) Which packet type is responsible for sending routing advertisements?

- A) ACK
- B) hello
- C) query
- D) reply
- E) update

Q3) Which packet type is used to acknowledge a reliable packet?

- A) ACK
- B) hello
- C) query
- D) reply
- E) update

Q4) Which packet type is used to respond to a query?

- A) ACK
- B) hello
- C) query
- D) reply
- E) update

Q5) Which packet type is used to ask neighbors about routing information?

- A) ACK
- B) hello
- C) query
- D) reply
- E) update

- Q6) Which three requirements are necessary to establish an EIGRP adjacency? (Choose three.)
- A) K values must match.
 - B) Neighbors must use the same autonomous system number.
 - C) Hello and hold timers must match.
 - D) Primary address of the adjacent routers must be in the same subnet.
- Q7) Which three packets must be explicitly acknowledged? (Choose three.)
- A) ACK
 - B) hello
 - C) reply
 - D) query
 - E) update
- Q8) After how many retransmissions is the EIGRP neighbor adjacency reset?
- A) 1
 - B) 15
 - C) 16
 - D) Never—EIGRP keeps on retransmitting until connection comes up
- Q9) In what order must the routers exchange the packets for the initial route discovery process to take place?
- A) hellos, updates, ACKs for the updates
 - B) hellos, ACKs for the hellos, updates
 - C) ACKs, hellos, updates
 - D) hellos, ACKs for the hellos, updates, ACKs for the updates
- Q10) Which command shows receipt and generation of the packet types, sequence numbers, and serial numbers but not the contents of the packets?
- A) **debug ip eigrp**
 - B) **debug eigrp packet**
 - C) **show ip eigrp topology**
 - D) **show ip eigrp interface**
- Q11) Which command shows the contents of a packet and the EIGRP processing between the topology and routing table?
- A) **debug ip eigrp**
 - B) **debug eigrp packet**
 - C) **show ip eigrp topology**
 - D) **show ip eigrp interface**

Quiz Answer Key

Q1) B

Relates to: EIGRP Packets

Q2) E

Relates to: EIGRP Packets

Q3) A

Relates to: EIGRP Packets

Q4) D

Relates to: EIGRP Packets

Q5) C

Relates to: EIGRP Packets

Q6) A, B, D

Relates to: Establishing Neighbors

Q7) C, D, E

Relates to: EIGRP Reliability, Transmission Policy, and Transport Mechanism

Q8) C

Relates to: EIGRP Reliability, Transmission Policy, and Transport Mechanism

Q9) A

Relates to: Initial Route Discovery in EIGRP

Q10) B

Relates to: Verifying EIGRP Connectivity Using debug Commands

Q11) A

Relates to: Verifying EIGRP Connectivity Using debug Commands

EIGRP DUAL

Overview

This lesson describes the EIGRP Diffusing Update Algorithm (DUAL). Important DUAL-specific terms, such as *successor* and *feasible successor*, are defined. The formula that DUAL uses to calculate a feasible successor is presented as well as the query process for DUAL when no feasible successor exists.

Relevance

Understanding how EIGRP discovers alternate pathways and selects primary and secondary routers during times of network instability is extremely important for efficient troubleshooting.

Objectives

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

- Explain how EIGRP DUAL automatically selects the best route (successor)
- Describe how EIGRP DUAL automatically selects the second-best route (feasible successor)
- Define how EIGRP performs route selection when no feasible successor is available
- Analyze the EIGRP query and update process

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- Knowledge of the Cisco router user interface
- Understanding of how to read an IP routing table
- Understanding of networking terms, numbering schemes, and topologies
- Understanding of how to interpret the contents, entries, and indicators in a Cisco routing table
- Understanding of how to verify basic router configurations using **show** and **debug** command output

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Selection of a Successor by DUAL**
- **Selection of a Feasible Successor by DUAL**
- **Selection When No Feasible Successor Is Available**
- **EIGRP Query Process**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-3

Selection of a Successor by DUAL

This topic describes the DUAL feature of EIGRP and explains the term *successor*.

EIGRP DUAL

Cisco.com

The DUAL finite state machine decision process is as follows:

- **Tracks all routes advertised by neighbors**
- **Selects loop-free path using a successor and remembers any feasible successors**
- **If the successor is lost, uses a feasible successor**
- **If there is no feasible successor, queries neighbors and recomputes a new successor**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-4

The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses distance information, known as a metric, to select efficient, loop-free paths. The lowest-cost route is calculated by adding the cost between the next-hop router and the destination—referred to as the advertised distance (AD)—to the cost between the local router and the next-hop router. The sum of these costs is referred to as the feasible distance (FD).

A successor is a neighboring router that forwards packets. This router has a least-cost path to a destination that is guaranteed not to be part of a routing loop. Multiple successors can exist if they have the same FD. By default, up to four successors can be added to the routing table.

The next-hop router for the backup path is called the feasible successor. To qualify as a feasible successor, a next-hop router must have an AD less than the FD of the current successor route.

If the route of the successor is not valid and a suitable feasible successor exists, the feasible successor replaces an invalid successor in the routing table without a recalculation. More than one feasible successor can be available at one time in the EIGRP topology table.

If the route of the successor is not valid but no suitable feasible successor exists, a recomputation must occur. This process determines a new successor. The amount of time it takes to recalculate the route affects the convergence time.

EIGRP Successor			
Cisco.com			
EIGRP Topology Table			
Network	FD (EIGRP Metric)	AD	EIGRP Neighbor
10.1.1.0 /24 10.1.1.0 /24	2000-Successor 2500	1000 1500	Router B (E0) Router D (E1)

IP Routing Table			
Network	Metric (FD)	Outbound Interface	Next Hop (EIGRP Neighbor)
10.1.1.0 /24	2000	Ethernet 0	Router B

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

The term *successor* refers to the best next-hop router to reach a given destination network. That router is chosen because it has the lowest FD of all possible pathways to that destination network. The successor is the next router in line to reach that destination or, in other words, the router with the best pathway to reach that destination network.

The router selects the best pathway to reach a given network. The router installs the destination network, the metric to reach that network, the outbound interface to reach the next-hop router, and the IP address of the next-hop router into the IP routing table. If there are a number of entries in the EIGRP topology table with an equal cost FD to a given destination network, all successors, up to four by default, for that destination network are installed in the routing table. AD does not have an effect on the selection of the best routes for incorporation in the routing table if EIGRP is the only routing protocol running on the router.

All routing protocols choose the next-hop router only. Each router counts on the next router to make a reliable decision to reach a specific destination network. The hop-by-hop pathway through a network goes from one router to the next. Each router makes a path selection on how to reach a given network and installs the best next-hop address along the pathway to reach that destination network. A router trusts the successor for a route (the best next-hop router) to send traffic towards that destination address.

Example

For example, in the figure, suppose that EIGRP router B advertises 10.1.1.0/24 to its EIGRP neighboring router C. The cost for router B to reach network 10.1.1.0/24 is 1000. Router C recognizes this value as the AD from router B. Router C must add its cost (1000) to reach router B and calculate the FD through router B to reach network 10.1.1.0/24, which is 2000 ($1000 + 1000$).

Router D advertises 10.1.1.0/24 to router C. The cost for router D to reach network 10.1.1.0/24 is 1500. Router C receives this cost as the AD from router D. Router C adds its cost (1000) to reach router D and calculate the FD through router D to reach network 10.1.1.0/24, which is

2500 ($1000 + 1500$). Router C compares all the FD for network 10.1.10/24 and then takes the lowest FD as the best route. Since the lowest FD is 2000, router C chooses to go to the next-hop router of router B to reach network 10.1.1.0/24. Router B is the successor (next available router) for router C to reach network 10.1.1.0/24.

Network 10.1.1.0/24 is installed in the IP routing table. The FD is the metric used by EIGRP in the routing table, and the next-hop address is the successor from the EIGRP topology table (router B).

Selection of a Feasible Successor by DUAL

This topic defines the feasible successor and explains the formula to select a feasible successor.

EIGRP Feasible Successor

Cisco.com

EIGRP Topology Table			
Network	FD (EIGRP Metric)	AD	EIGRP Neighbor
10.1.1.0 /24	2000-Successor 2500	1000 1500 Feasible Successor	Router B (E0) Router D (E1)
10.1.1.0 /24			

AD of second-best route < FD of best route (successor) = feasible successor

If the above equation is true, a loop-free pathway through the feasible successor exists; automatically switch to the feasible successor on failure of the best route (successor).

D145_117

© 2004 Cisco Systems, Inc. All rights reserved.

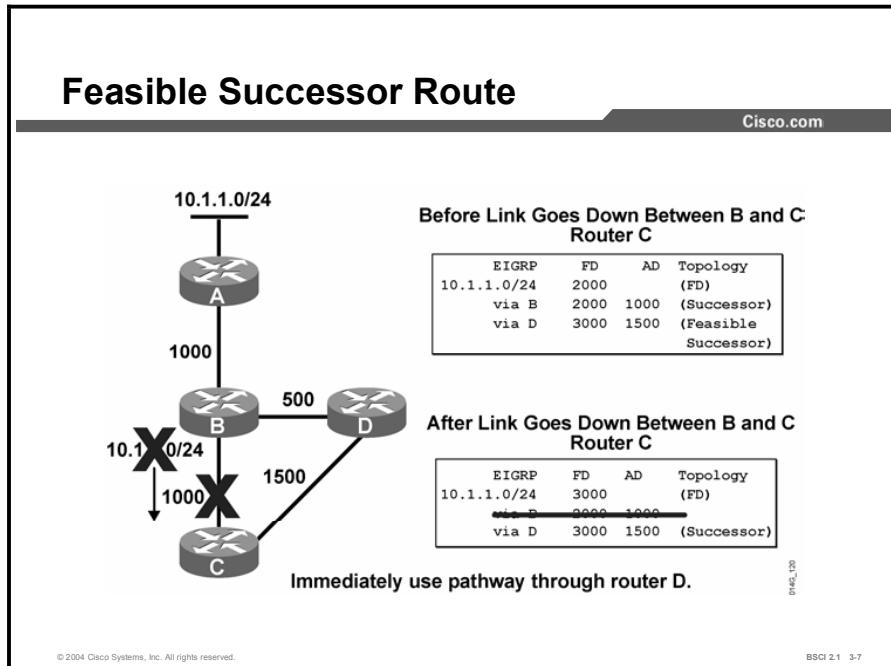
BSCI 2.1 3-6

Backup routes, called *feasible successors*, are selected at the same time that the successors are identified. These feasible successor routes are in the topology table. The topology table can retain multiple feasible successors for a destination. A feasible successor is a destination address that is loop-free, or that does not loop back to the current successor. By definition, a feasible successor must be mathematically proven.

A feasible successor is selected by comparing the AD of a nonsuccessor route to the FD of the best route. If the AD of the nonsuccessor route is less than the FD of best route, then that route is identified as a feasible successor. If the successor becomes unavailable, then the feasible successor can be used immediately, without recalculating for a lost route.

The equation in the figure illustrates this process.

Example



In the figure, the link between router B and router C fails. Router C removes route 10.1.1.0/24 through router B from the routing table and searches the EIGRP topology table for a feasible successor. Since router D can still reach the network and does not send an update or query packet to inform router C of the lost route, router C immediately uses the pathway through router D. Router C chooses this path because the AD of router D is less than the FD to reach router B. The mathematical proof verifies that there is no routing loop that uses this pathway.

Selection When No Feasible Successor Is Available

This topic examines instances when EIGRP cannot mathematically determine a feasible successor and provides an example of what happens without the DUAL discovery process.

No EIGRP Feasible Successor

Cisco.com

EIGRP Topology Table			
Network	FD (EIGRP Metric)	AD	EIGRP Neighbor
10.1.1.0 /24 10.1.1.0 /24	2000-Successor 3000	1000 2000 No Feasible Successor	Router B (E0) Router D (E1)

AD of second-best route \geq FD of best route (successor) \neq feasible successor

If the above equation is true, no feasible successor exists, and the discovery process must be executed for any lost routes.

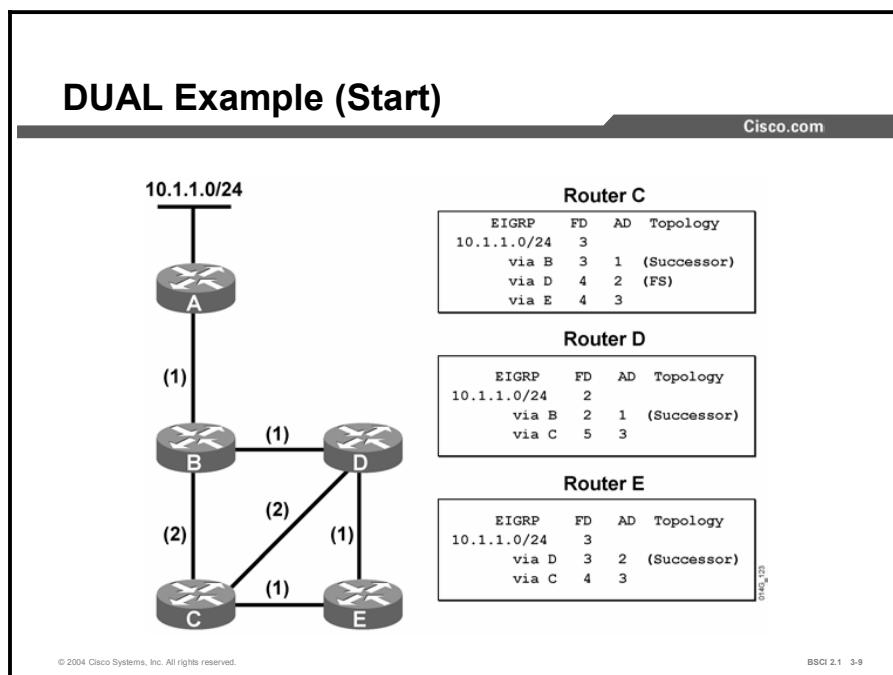
© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

The mathematical formula to ensure that the feasible successor is loop-free requires that the AD of the second-best route be *less than* the FD of the successor. When the AD of the second-best route is greater than or equal to the FD of the successor, a feasible successor cannot be chosen. In this case, a discovery process that uses EIGRP queries and replies must be used to find any alternate pathways to the lost networks.

EIGRP Query Process

This topic provides a detailed walk-through of the EIGRP query and reply process.



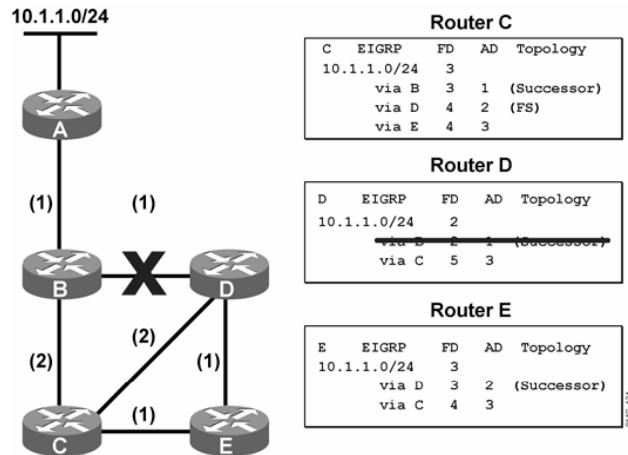
In the figure, the topology table indicates the following:

- **FD:** The feasible distance that equals the sum of the costs of the links to reach network 10.1.1.0/24
- **AD:** The advertised distance that equals the sum of the costs of the links to reach network 10.1.1.0/24 as advertised by neighboring routers
- **Successor:** The forwarding path used to reach network 10.1.1.0/24. The path cost to network 10.1.1.0 is the FD
- **Feasible successor:** An alternate loop-free backup path to reach network 10.1.1.0

Note The sample network is stable and converged. All the routes are in the passive state. EIGRP uses the split horizon feature. For example, router E does not pass its route to reach network 10.1.1.0/24 back to router D, because router E uses router D as its next hop to network 10.1.1.0/24.

DUAL Example: Link Goes Down

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-10

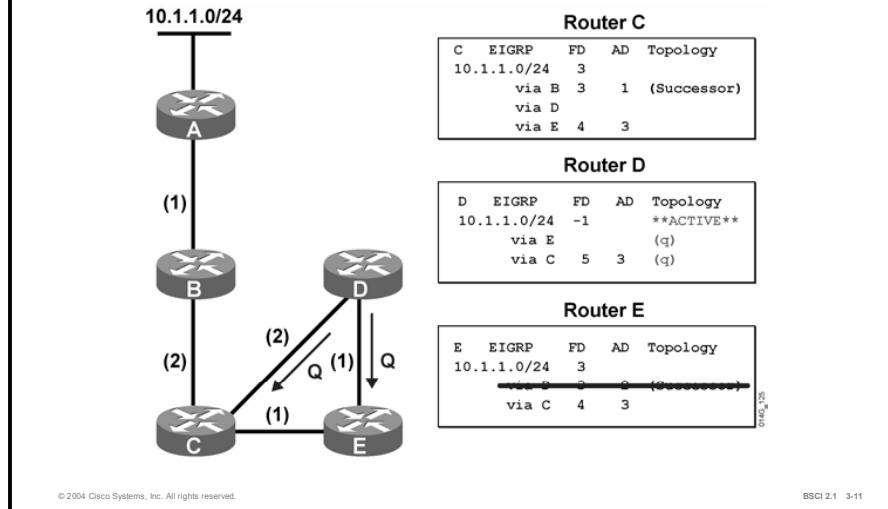
In the figure, routers B and D detect a link failure.

Upon notification of the link failure, DUAL performs the following steps, as illustrated in the figures that follow:

- Step 1** At router D, DUAL marks the path to network 10.1.1.0/24 through router B as unusable.

DUAL Example: D Sends Queries

Cisco.com



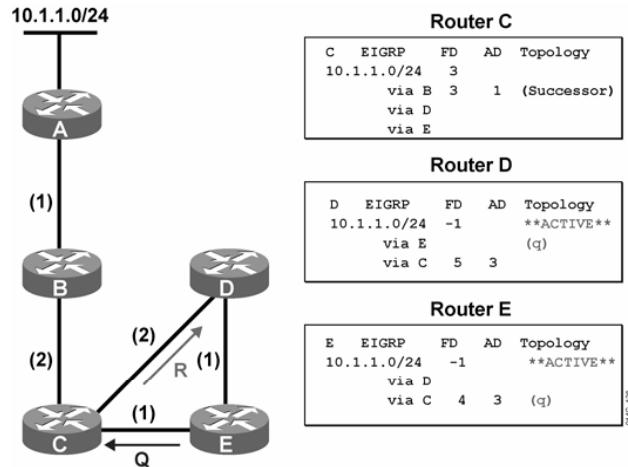
Step 2 At router D: DUAL has no feasible successor to network 10.1.1.0/24, because the AD via router C (3) is greater than the FD via router B (2).

1. DUAL sets the metric to network 10.1.1.0/24 as unreachable (-1 is unreachable). A feasible successor cannot be found in the topology table, and the route changes from the passive state to the active state. In the active state, the router sends queries to neighboring routers looking for a new successor.
2. It sends a query to routers C and E to look for an alternate path to network 10.1.1.0/24.
3. It marks routers C and E as having a query (Q in the figure) pending.

Step 3 At router E: DUAL marks the path to network 10.1.1.0/24 through router D as unusable.

DUAL Example: E Sends Queries

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-12

Step 4 At router D: DUAL receives a reply from router C that indicates no change for the path via router C to reach network 10.1.1.0/24.

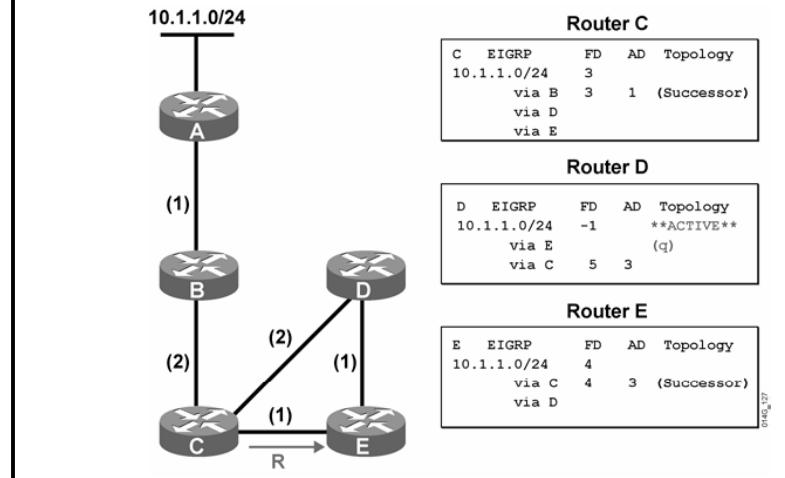
1. It removes the query flag from router C.
2. It remains active on network 10.1.1.0/24, still waiting for a reply from router E to its query.

Step 5 At router E: DUAL has no feasible successor to network 10.1.1.0/24. The route to network 10.1.1.0/24 becomes active.

1. DUAL generates a query to router C.
2. It marks router C as having a query pending.

DUAL Example: C Replies

Cisco.com



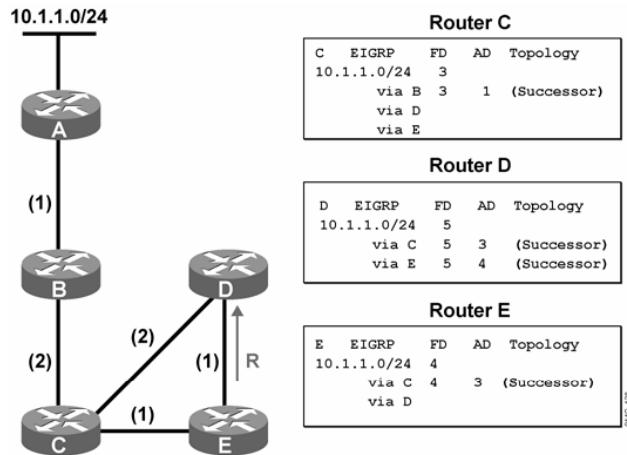
Step 6 At router D: DUAL stays active on network 10.1.1.0/24, still waiting for a reply to its query from router E.

Step 7 At router E: DUAL receives a reply from router C that indicates no change.

1. It removes the query flag from router C.
2. It calculates a new FD and installs a new successor route in the topology table.
3. It changes the route to network 10.1.1.0/24 from active to passive (converged).

DUAL Example: E Replies

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

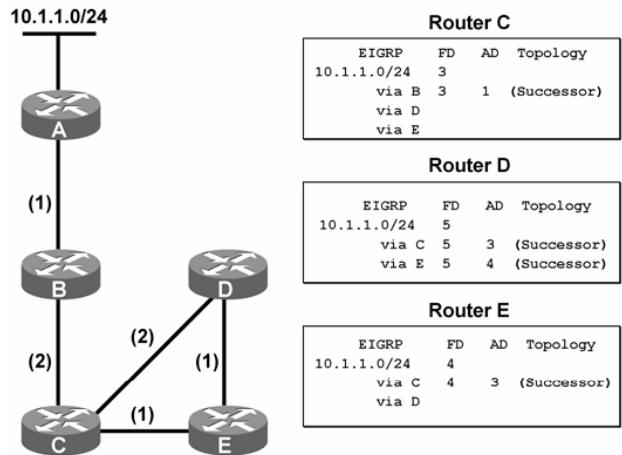
BSCI 2.1 3-14

Step 8 At router D: DUAL receives a reply from router E.

1. It removes the query flag from router E.
2. It calculates a new FD.
3. It installs new successor routes in the table. Because both routes (via routers C and E) have the same FD, both are marked as successors. The route to network 10.1.1.0/24 changes from active to passive (converged).

DUAL Example: Convergence

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-15

At router D, two successor routes exist in the topology table for network 10.1.1.0/24. Both successor routes are listed in the routing table, and equal-cost load balancing is in effect.

The network is stable and converged.

Notice that throughout the entire convergence process, only routes to network 10.1.1.0/24 become active on routers D and E. The route to network 10.1.1.0/24 on router C remains passive because the link failure between routers B and D does not affect the successor route from router C to network 10.1.1.0/24.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **DUAL is a finite-state formula that uses a discovery process to calculate loop-free routes.**
- **EIGRP labels the best pathway to a given network as the successor.**
- **If the AD of a nonsuccessor route is less than the feasible distance of the best route, that route is labeled as the feasible successor and can be used immediately if the pathway through the successor for a network becomes unavailable.**
- **If there is no feasible successor for a given network and the pathway through the successor becomes unavailable, a query-and-reply process is automatically executed to find a loop-free pathway to the lost network.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-16

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 DUAL select the successor for a specific destination network?
- A) by selecting the next-hop router with the highest FD
 - B) by selecting the next-hop router with the lowest FD
 - C) by selecting the next-hop router with the highest AD
 - D) by selecting the next-hop router with the lowest AD
- Q2) What is the formula for selecting a feasible successor?
- A) The AD of the successor is less than the FD of the nonsuccessor route.
 - B) The FD of the successor is less than the AD of the nonsuccessor route.
 - C) The FD of the nonsuccessor route is less than the AD of the successor.
 - D) The AD of the nonsuccessor route is less than the FD of the successor.
- Q3) When EIGRP cannot determine a feasible successor, but alternate pathways exist and the successor becomes unavailable, what does EIGRP do?
- A) It immediately uses the alternate pathway with the lowest FD and sends queries and updates to ensure that this pathway is loop-free.
 - B) It automatically uses the alternate pathway with the lowest FD.
 - C) It performs queries and updates to see if the alternate pathways are still viable. When a loop-free path is found, the path is installed in the routing table.
 - D) It removes the network from the routing table and waits for the periodic update from EIGRP neighbors to see if an alternate route exists.
- Q4) Which two conditions signify the active state for EIGRP? (Choose two.)
- A) The route can be used and is stable.
 - B) The route cannot be used.
 - C) EIGRP queries are outstanding and the router is waiting for EIGRP replies.
 - D) The state signifies that this is the best route with the lowest FD.

Quiz Answer Key

Q1) B

Relates to: Selection of a Successor by DUAL

Q2) D

Relates to: Selection of a Feasible Successor by DUAL

Q3) C

Relates to: Selection When No Feasible Successor Is Available

Q4) B, C

Relates to: EIGRP Query Process

Configuring and Verifying EIGRP

Overview

This lesson explains and demonstrates how to configure basic EIGRP. This lesson also explains how to use a default network with EIGRP and how to use the wildcard option for a network mask. To assist in troubleshooting, this lesson introduces various Cisco IOS software **show** commands and defines the key fields in each.

Relevance

Knowing the correct commands to use when you configure EIGRP ensures that migration to this routing protocol is smooth and quick. Understanding which **show** command to use when troubleshooting the EIGRP configuration saves valuable time.

Objectives

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

- Configure EIGRP
- Configure a default route using the **default-network** command
- Verify EIGRP using **show** commands

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience
- An understanding of how to operate and configure a Cisco router
- An understanding of how to verify basic router configurations using **show** and **debug** command output

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Configuring EIGRP**
- **Configuring Default Route Using the default-network Command**
- **Verifying EIGRP Using show Commands**
- **Summary**
- **Quiz**

Configuring EIGRP

This topic defines the commands used to configure basic EIGRP and presents two examples of these commands.

Configuring EIGRP

Cisco.com

Router (config) #

router eigrp autonomous-system-number

- Defines EIGRP as the IP routing protocol.
- All routers in the internetwork that must exchange EIGRP routing updates must have the same autonomous system number.

Router (config-router) #

network network-number [wildcard-mask]

- Identifies attached networks participating in EIGRP.
- **wildcard-mask:** An inverse mask used to determine how to read the address. The mask has wildcard bits, where 0 is a match and 1 is “don’t care.”

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-4

To configure EIGRP for IP, perform the following steps:

- Step 1** Enable EIGRP and define the autonomous system using the **router eigrp autonomous-system** command. The autonomous system number value must match on all routers within the autonomous system.
- Step 2** Indicate which networks are part of the EIGRP autonomous system using the **network network-number** command. This command determines which interfaces of the router are participating in EIGRP and which networks the router advertises.

If you do not use the optional wildcard mask, the EIGRP process assumes that all directly connected networks that are part of the overall major network will participate in the EIGRP routing process. In the EIGRP routing process, EIGRP packets attempt to establish EIGRP neighbor relationships from each interface that is part of the overall Class A, B, or C network.

Use the optional wildcard mask to identify the specific IP address, subnet, or network. The router interprets the network number by comparing it to the wildcard mask to determine which connected networks will participate in the EIGRP routing process.

Network area Command	Description
<i>network-number</i>	This command can be the network address, subnet, or the address of the interface. It instructs the router to recognize which links to advertise to, which links to listen to advertisements on, and which networks to advertise.
<i>Wildcard-mask</i>	<p>An inverse mask used to determine how to read the address. The mask has wildcard bits, where 0 is a match and 1 is don't care. For example, 0.0.255.255 indicates a match in the first two bytes.</p> <p>If specifying the interface address, use the mask 0.0.0.0 to match all four bytes of the address.</p> <p>An address and wildcard mask combination of 0.0.0.0 255.255.255.255 matches all interfaces on the router.</p>

- Step 3** If you are using serial links, define the bandwidth of a link on which to send routing update traffic. If you do not change the bandwidth for these interfaces, EIGRP assumes that the bandwidth on the link is equivalent to T1 speed. If the link is slower, the router cannot converge, or routing updates might become lost. Define the bandwidth of the link using the **bandwidth kilobits** command. For example, for a 64-kbps link, use the following command:

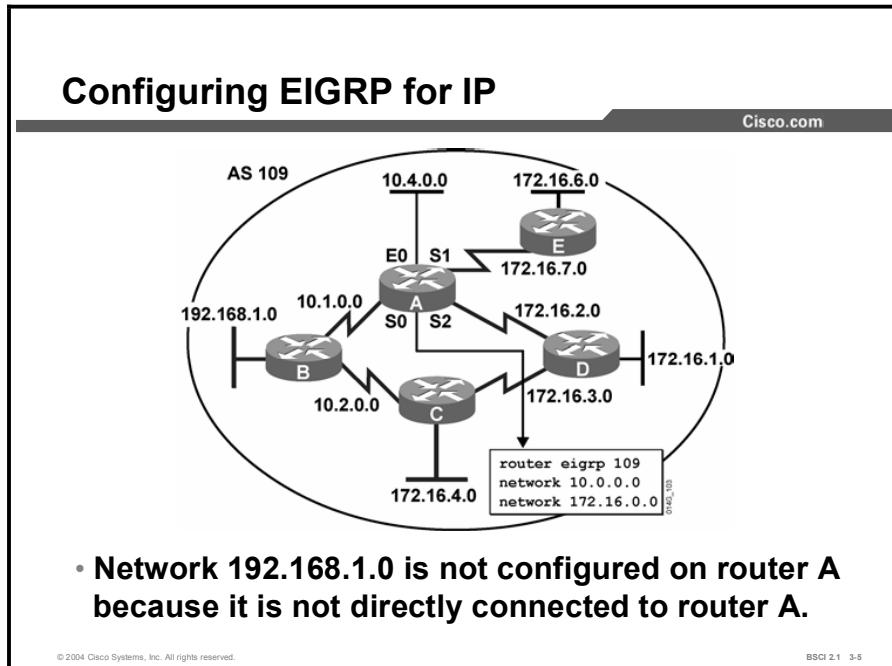
```
router(config-if)# bandwidth 64
```

Bandwidth kilobits represent the intended bandwidth, measured in kilobits. For generic serial interfaces, such as PPP or HDLC, set the bandwidth to the line speed.

For Frame Relay on point-to-point interfaces, set the bandwidth to the committed information rate (CIR).

For Frame Relay multipoint connections, set the bandwidth to the sum of all CIRs or, if the permanent virtual circuits (PVCs) have different CIRs, then set the bandwidth to the lowest CIR multiplied by the number of PVCs for the multipoint connection.

Example



The figure illustrates the configuration of router A for EIGRP. Router A, along with all routers in the figure, is part of autonomous system 109. For EIGRP to establish a neighbor relationship, all neighbors must be in the same autonomous system.

Because the wildcard mask is not used, all interfaces on router A that are part of network 10.0.0.0/8 and network 172.16.0.0/16 participate in the EIGRP routing process.

One option for router A is the following configuration:

```
routerA(config)# router eigrp 109
routerA(config-router)# network 10.1.0.0
routerA(config-router)# network 10.4.0.0
routerA(config-router)# network 172.16.7.0
routerA(config-router)# network 172.16.2.0
```

The router summarizes the **network** commands to the classful networks automatically and the resulting configuration resembles the following:

- **router eigrp 109**
- **network 10.0.0.0**
- **network 172.16.0.0**

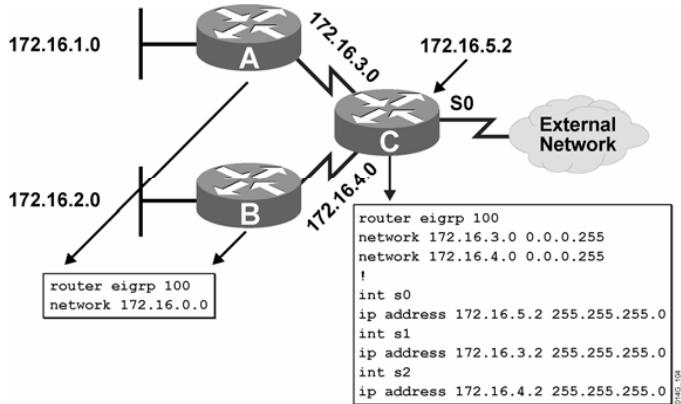
Another option for router A is the following configuration:

```
routerA(config)# router eigrp 109
routerA(config-router)# network 10.1.0.0 0.0.255.255
routerA(config-router)# network 10.4.0.0 0.0.255.255
routerA(config-router)# network 172.16.2.0 0.0.0.255
routerA(config-router)# network 172.16.7.0 0.0.0.255
```

The router matches the network number with the wildcard mask to determine which directly connected interfaces participate in the EIGRP routing process for autonomous system 109. In this case, all interfaces that are part of network 10.1.0.0/16, 10.4.0.0/16, 172.16.2.0/24, and 172.16.7.0/24 participate in the EIGRP routing process for autonomous system 109.

Using the Wildcard Mask in EIGRP

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

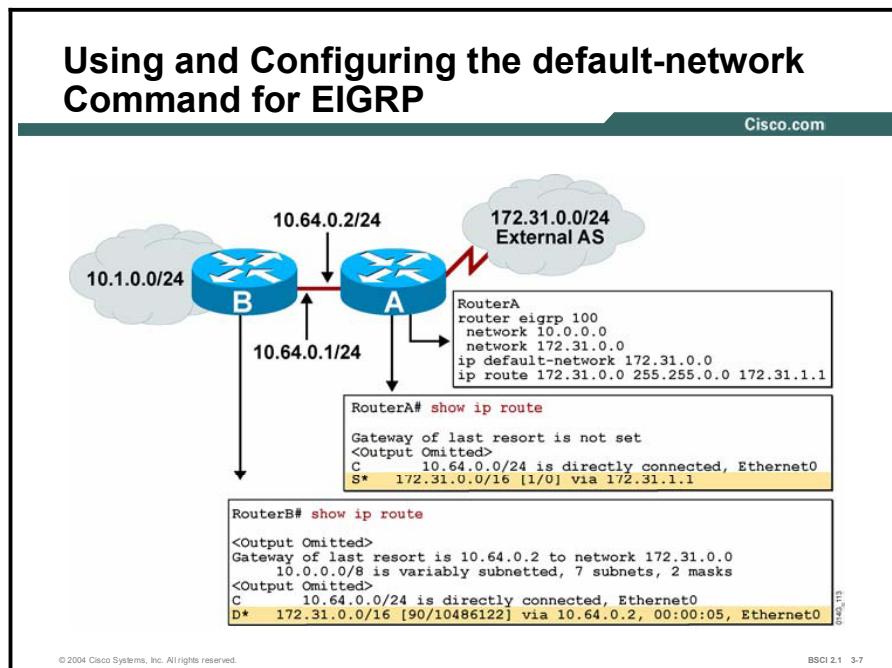
BSCI 2.1 3-6

The configuration in the figure uses the wildcard mask, because router C connects to a router external to this network. The other internetwork can also run EIGRP with the same autonomous system, although this approach is unlikely.

The router C configuration includes subnets of the Class B network 172.16.0.0 on all interfaces. Without the wildcard mask, router C sends EIGRP packets to the external network, which wastes bandwidth and CPU cycles and provides unnecessary information to an external network. The wildcard mask tells EIGRP to establish a relationship with EIGRP routers from an IP interface that is part of network 172.16.3.0/24 or 172.16.4.0/24 and not 172.16.5.0/24.

Configuring Default Route Using the default-network Command

This topic demonstrates how to configure a default route for the EIGRP process so that it propagates to other EIGRP routers within the same autonomous system.



When you use EIGRP, create the default route with the **ip default-network network-number** command. A router configured with the **ip default-network** command for EIGRP considers the network listed in that command as the last-resort gateway. The network must be reachable by the router that uses this command before it announces it as a candidate default route to other EIGRP routers. The network configuration in this command must also be passed to other EIGRP routers so that those routers can use this network as their default network and set the gateway of last resort pointing at this default network. This approach means that the network must be an EIGRP-derived network in the routing table, or the static route used to generate the route to the network must be redistributed into EIGRP.

Multiple default networks can be flagged, and downstream routers use the EIGRP metric to determine the best default route.

In the figure shown, router A is directly attached to external network 172.31.0.0/16. Router A flags the 172.31.0.0 network as a candidate default network with the **ip default-network 172.31.0.0** command. The network passes to router B because router A has that network listed in a **network** command under the EIGRP process. The routing table for router A does not set the gateway of last resort. The **ip default-network** command does not benefit router A directly. On router B, it flags the EIGRP-learned 172.31.0.0 network as a candidate default network. It also sets the gateway of last resort as 10.64.0.2 to reach the default network of 172.31.0.0.

Command	Description
ip default-network	A method to distribute default route information to other routers via EIGRP. This command provides no functionality for the router on which it is configured.
network-number	The number of the classful destination network.

Note	EIGRP and Interior Gateway Routing Protocol (IGRP) behave differently from Routing Information Protocol (RIP) with the ip route 0.0.0.0 0.0.0.0 command. For example, EIGRP does not understand and pass the 0.0.0.0 0.0.0.0 route by default. However, if the network 0.0.0.0 command is added to the EIGRP configuration, it will pass a default route as the result of the ip route 0.0.0.0 0.0.0.0 command. The 0.0.0.0 0.0.0.0 static default route can also be redistributed into EIGRP.
-------------	---

The following shows an example:

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
router eigrp 100
network 0.0.0.0 (or redistribute static)
```

Verifying EIGRP Using show Commands

This topic explains and demonstrates the use of various Cisco IOS software **show** commands to verify the EIGRP configuration.

Verifying EIGRP: show ip route

Cisco.com

```
RouterA# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
       D - EIGRP, EX - EIGRP external, O - OSPF,
       (text omitted)
       * - candidate default,
Gateway of last resort is not set
    172.16.0.0/24 is subnetted, 1 subnets
D      172.16.1.0 [90/10639872] via 10.1.2.2, 06:04:01, Serial0/0
          10.0.0.0/24 is subnetted, 4 subnets
D        10.1.3.0 [90/10514432] via 10.1.2.2, 05:54:47, Serial0/0
D        10.3.1.0 [90/10639872] via 10.1.2.2, 06:19:41, Serial0/0
C        10.1.2.0 is directly connected, Serial0/0
C        10.1.1.0 is directly connected, Ethernet0/0
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

To verify that the router recognizes EIGRP routes for any neighbors, use the **show ip route** command.

The **show ip route** command displays all the routes in the routing table. EIGRP routes are identified with a D in the left column. Notice that after each EIGRP network number there is a field that looks similar to 90/10639872. The second number in the string may be different from the one in the example.

The router uses the first number, 90, as the default AD to determine preference for a route. Consider that this router also uses RIP. In this example, RIP has a route to network 10.1.3.0 that is three hops away. The router, without AD, cannot compare three hops to an EIGRP metric of 10639872. The router does not know the bandwidth associated with hops, and EIGRP does not use hop count as a metric.

To correct this problem, Cisco established an AD value for each routing protocol, and by default, gave EIGRP internal routes an AD of 90. RIP has an AD of 120. Because EIGRP has a better metric based upon bandwidth and delays, it is preferred over RIP. As a result, the EIGRP route is installed in the routing table.

The second number in the string is the EIGRP metric, which equals the EIGRP-calculated least-cost bandwidth plus the EIGRP-calculated delay. The EIGRP metric number is the same number found in the EIGRP topology table for this network as the FD.

The 10.1.2.2 address for each EIGRP entry is the next-hop router to which this router passes the packets. The packet destination is a network behind that next hop. The next-hop address in the preceding figure is the same as the successor in the EIGRP topology table.

Each route also has a time stamp associated with it. The time stamp is the length of time, perhaps days or months, since EIGRP last advertised this network to this router. EIGRP does not refresh routes periodically. It resends the routing database only when neighbor adjacencies change.

Verifying EIGRP: show ip protocols

Cisco.com

```
RouterA# show ip protocols

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  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 not in effect
  Maximum path: 4
  Routing for Networks:
    10.1.0.0/16
    10.0.0.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    10.1.2.2          90           05:50:13
  Distance: internal 90 external 170
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

Use the **show ip protocols** command to examine default EIGRP settings. The command output displays any routing filtering occurring on EIGRP outbound or inbound updates. It also identifies if EIGRP is generating a default network or receiving a default network in EIGRP updates.

The command output provides information about additional default settings for EIGRP, such as default K values, hop count, and variance.

Note	Because the routers must have identical K values for EIGRP to establish an adjacency, the show ip protocols command helps to determine the current K value setting before an adjacency is attempted.
-------------	---

This sample output also indicates that automatic summarization is disabled and that the router is allowed to load-balance over a maximum of four paths. The EIGRP process allows configuration of up to six pathways for equal-cost load balancing. Use the **maximum-path** command for this purpose.

The router routes for networks 10.1.0.0/16 and 10.0.0.0. Therefore, you can configure the following network commands:

- **router eigrp 100**
- **network 10.1.0.0 0.0.255.255**
- **network 10.0.0.0**

Results vary depending on the use of the wildcard mask statement used with the address. When you use the wildcard mask, the network address displays with the prefix length of the bits EIGRP matched to send updates from that interface. When you use no wildcard mask, this command displays the Class A, B, or C major network.

The routing information source portion of this command identifies all other routers that have an EIGRP neighbor relationship with this router. The **show ip eigrp neighbor** command provides a detailed display of EIGRP neighbors.

The **show ip protocols** command output also provides the ADs for EIGRP. EIGRP has two ADs. First, an AD of 90 applies to networks from other routers inside the autonomous system number. These are considered internal networks for this autonomous system. Second, an AD of 170 applies to networks introduced to EIGRP for this autonomous system through redistribution. These are termed external networks.

Verifying EIGRP: show ip eigrp topology

Cisco.com

```
RouterA# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(10.1.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
          r - reply Status, s - sia Status
P 10.1.3.0/24, 1 successors, FD is 10514432
    via 10.1.2.2 (10514432/28160), Serial0/0
P 10.3.1.0/24, 1 successors, FD is 10639872
    via 10.1.2.2 (10639872/384000), Serial0/0
P 10.1.2.0/24, 1 successors, FD is 10511872
    via Connected, Serial0/0
P 10.1.1.0/24, 1 successors, FD is 2190
    via Connected, Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 10639872
    via 10.1.2.2 (10639872/384000), Serial0/0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-10

The last command used to verify EIGRP operations is the **show ip eigrp topology** command. The command output lists the networks known by this router through the EIGRP routing process. For example, the figure illustrates a router (10.1.2.1) in autonomous system 100. The EIGRP ID is the highest IP address on an active interface for this router. The codes are as follows:

- **Passive:** This network is available and installation can occur in the routing table. Passive is the correct state for a stable network.
- **Active:** This network is currently unavailable and installation cannot occur in the routing table. This means that there are outstanding queries for this network.
- **Update (U):** This code applies if a network is being updated (placed in an update packet). This code also applies if the router is waiting for an acknowledgment for this update packet.
- **Query (Q):** This code applies if there is an outstanding query packet for this network other than being in the active state. This code also applies if the router is waiting for an acknowledgment for a query packet.
- **Reply (R):** This code applies if the router is generating a reply for this network or is waiting for an acknowledgment for the reply packet.
- **Stuck-in-active (SIA) status:** This code signifies an EIGRP convergence problem for the network with which it is associated.

In the example, each network has the number of successors available for that route. All networks have one successor, but if there were equal-cost pathways to the same network, a maximum of six paths are allowed. The number of successors corresponds to the number of best routes with equal cost. The routing table contains all the equal-cost best routes, up to six for the same network. For each network, the FD is listed next, followed by the next-hop address listed at the beginning of the second line.

After the next-hop address is a field that looks similar to 10639872/384000. The first number is the FD for that network, and the second number is the advertised distance. The next-hop router advertised this distance to the router.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The configuration commands for basic implementation include:**
 - `router eigrp autonomous-system`
 - `network network-number [wildcard-mask]`
- **Create and advertise a default route in an EIGRP autonomous system with the following command:**
 - `ip default-network reachable-network-number`
- **The Cisco IOS show commands to verify correct configuration and operation of EIGRP include:**
 - `show ip route`
 - `show ip protocols`
 - `show ip eigrp topology`

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-11

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 3-1: Configuring and Tuning EIGRP

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 **network** command for EIGRP?
- A) to determine which router interfaces participate in EIGRP and which networks the router advertises
 - B) to specify the autonomous system number to which the router belongs
 - C) to define the EIGRP neighbors
 - D) to tell EIGRP which networks to advertise, those directly connected and those learned through EIGRP
- Q2) Which command creates a default route for EIGRP?
- A) **ip default-network network-number**
 - B) **ip route 0.0.0.0 0.0.0.0 outbound-interface**
 - C) **ip route 0.0.0.0 255.0.0.0 outbound-interface**
 - D) **ip route 0.0.0.0 255.255.255.255 outbound-interface**
- Q3) Which command displays a network that is SIA?
- A) **show ip route**
 - B) **show ip protocol**
 - C) **show ip eigrp topology**
- Q4) Which command displays the K value settings for EIGRP?
- A) **show ip route**
 - B) **show ip protocol**
 - C) **show ip eigrp topology**

Quiz Answer Key

Q1) A

Relates to: Configuring EIGRP

Q2) A

Relates to: Configuring Default Route Using the default-network Command

Q3) C

Relates to: Verifying EIGRP Using show Commands

Q4) B

Relates to: Verifying EIGRP Using show Commands

Advanced EIGRP Configuration Options

Overview

For a scalable EIGRP network, configuring manual route summarization at key points on the internetwork is vital to good network performance.

Large networks use redundant links in their cores. This lesson provides advanced configuration options for EIGRP, including load balancing, manual route summarization, and limiting EIGRP bandwidth utilization on WAN links.

Relevance

Load balancing across multiple links is a viable option for efficient bandwidth utilization. Limiting the amount of bandwidth that EIGRP uses across these WAN links allows user traffic better access to the WAN links.

Objectives

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

- Describe and configure EIGRP manual route summarization
- Describe and configure load balancing across equal paths
- Describe and configure unequal-cost load balancing in EIGRP using the **variance** command
- Describe and configure EIGRP bandwidth utilization on WAN links

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **EIGRP Manual Route Summarization**
- **Understanding EIGRP Load Balancing**
- **Load Balancing Across Unequal-Cost Paths Using Variance**
- **EIGRP Bandwidth Utilization**
- **Summary**
- **Quiz**

EIGRP Manual Route Summarization

This topic describes how EIGRP performs autosummarization by default. This topic also provides information on the method to perform manual summarization and an example of its use.

EIGRP Route Summarization: Automatic

Cisco.com

- **Purpose: Smaller routing tables, smaller updates, query boundary**
- **Autosummarization:**
 - On major network boundaries, subnetworks are summarized to a single classful (major) network.
 - Autosummarization occurs by default.

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-4

Some features of EIGRP are characteristic of pure distance vector operation. Automatic route summarization at major network boundaries is an example of traditional distance vector behavior. Traditional distance vector protocols, which are classful routing protocols, cannot assume the mask for networks that are not directly connected because routing updates do not exchange routing masks.

In addition to the restrictions imposed by the lack of mask information, summarizing routes at major classful boundaries creates smaller routing tables. Smaller routing tables make the routing update process less bandwidth-intensive. Autosummarization is enabled by default for EIGRP.

EIGRP Route Summarization: Manual

Cisco.com

Manual summarization has the following characteristics:

- **Summarization is configurable on a per-interface basis in any router within a network.**
- **When summarization is configured on an interface, the router immediately creates a route pointing to null0.**
 - **Loop prevention mechanism**
- **When the last specific route of the summary goes away, the summary is deleted.**
- **The minimum metric of the specific routes is used as the metric of the summary route.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

A drawback to using distance vector protocols is the inability to create summary routes at arbitrary boundaries in a major network. EIGRP allows administrators to disable autosummarization and to create one or more summary routes within the network.

When a network administrator creates a summary route, that route is added to the routing table with a reference to null 0, which is a directly connected, software-only interface. The null 0 interface prevents the router from trying to forward traffic to other routers in search of a more precise, longer match contained within the aggregated route. This feature prevents traffic from looping within the network. For example, if the summarizing router receives a packet to an unknown subnet that is part of the summarized range, the packet matches the summary route based on the longest match. The packet is forwarded to the null 0 interface (the bit bucket). This prevents the router from forwarding the packet to a default route and possibly creating a loop.

For manual summarization to be effective, blocks of contiguous addresses (subnets) must come together at a common router so that the router can advertise a single summary route at the interface level. The formula 2^n , where n equals the number of bits by which the subnet mask has been reduced, indicates how many subnets a single summary route can represent. For example, if the summary mask contains three fewer bits than the subnet mask, eight subnets can be aggregated into one advertisement.

When the summarization block is 10.1.8.0/21 and the network 10.0.0.0 is divided into /24 subnets, the difference between the /24 networks and the /21 summarizations is 3 bits, and $2^3 = 8$. The summarized subnets range from 10.1.8.0/24 through 10.1.15.0/24.

When specifying summary routes, the administrator needs to specify the IP address only of the summary route and the routing mask. Cisco IOS software for EIGRP handles many of the details that surround proper implementation, including details about metrics, loop prevention, and removal of the summary route from the routing table if none of the more specific routes are valid.

Configuring Route Summarization

Cisco.com

```
(config-router) #
```

```
no auto-summary
```

- Turns off autosummarization for the EIGRP process

```
(config-if) #
```

```
ip summary-address eigrp [as-number]  
[address] [mask]
```

- Creates a summary address this interface will generate

© 2004 Cisco Systems, Inc. All rights reserved.

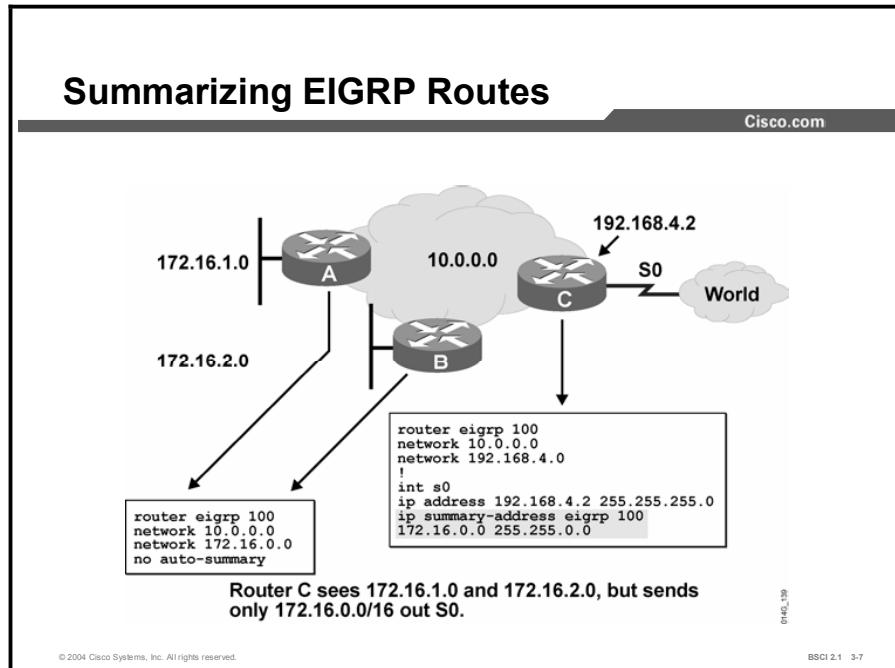
BSCI 2.1 3-6

EIGRP automatically summarizes routes at the classful boundary. In some cases, however, you may not want autosummarization to occur. For example, if you have discontiguous networks, you need to disable autosummarization to minimize router confusion. To disable autosummarization, use the **no auto-summary** command under the EIGRP router configuration mode.

Use the **ip summary-address eigrp** interface command to manually create a summary route at an arbitrary network boundary within an EIGRP domain.

ip summary-address eigrp Command	Description
as-number	EIGRP autonomous system number.
address	The IP address advertised as the summary address. This address does not need to be aligned on Class A, B, or C boundaries.
mask	The IP mask used to create the summary address.

Example



In the configuration example, routers A and B have disabled autosummarization for the 172.16.1.0 and 172.16.2.0 subnets because those advertisements pass into network 10.0.0.0. The routing tables of routers in the 10.0.0.0 network now include these discontiguous subnets. At router C, the administrator creates a manual summary route to represent all subnets that belong to network 172.16.0.0 as a single entry in its advertisements to other networks. Router C will not autosummarize the 172.16.1.0 and 172.16.2.0 subnets because it does not own the 172.16.0.0 network. To configure manual route summarization, use the following procedure:

- Step 1** Select the interface to propagate the summary route.
- Step 2** Specify the summary address, the EIGRP routing protocol, and the autonomous system number of the routes being summarized.

Note For manual route summarization, the summary route is advertised only if a component (a more specific entry) of the summary route is present in the routing table.

Understanding EIGRP Load Balancing

This topic explains how EIGRP performs equal-cost path load balancing.

EIGRP Load Balancing

Cisco.com

- **Routes with a metric equal to the minimum metric are installed in the routing table (equal-cost load balancing).**
- **There can be up to six entries in the routing table for the same destination:**
 - The number of entries is configurable.
 - The default is four.
 - Set the routing table to one entry to disable load balancing.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

Load balancing occurs when a router distributes traffic over all its network ports that are the same distance from the destination address. Load balancing increases the use of network segments, and increases effective network bandwidth.

For IP, Cisco IOS software applies load balancing between equal-cost paths by default. When a packet is process-switched, load balancing over equal-cost paths occurs on a per-packet basis. When packets are fast-switched, load balancing over equal-cost paths occurs on a per-destination basis. Remember, for testing, do not ping to or from the routers with the fast-switching interfaces, because these locally router-generated packets are process-switched rather than fast-switched and might produce confusing results.

Load Balancing Across Unequal-Cost Paths Using Variance

This topic explains how to configure EIGRP unequal-cost path load balancing. It provides an example of unequal-cost load balancing.

EIGRP Unequal-Cost Load Balancing

Cisco.com

- **EIGRP offers unequal-cost load balancing.**
- **Variance allows the router to include routes with a metric smaller than the multiplier times the minimum metric route to that destination**
 - **Multiplier is the number specified by the variance command**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-9

EIGRP can balance traffic across multiple routes that have different metrics. The degree to which EIGRP performs load balancing is controlled with the **variance** command.

The multiplier is a variance value from 1 to 128, and it is used for load balancing. The default is 1, which indicates equal-cost load balancing. The multiplier defines the range of metric values that are accepted for load balancing by the EIGRP process.

Example

Variance Example

Cisco.com

The diagram shows a network topology with five routers (A, B, C, D, E) and a destination network labeled "Network Z". Router E is configured with a variance of 2. The link costs between routers are: E-B (20), E-C (10), C-B (10), C-A (10), C-D (30), and D-A (15). Router E has two paths to Network Z: one through router C (cost 20 + 10 = 30) and one through router B (cost 20). Since the variance is 2, router E can choose router B as an alternate path to Network Z because $2 * (FD) = 40$ is greater than the cost of 30. Router D is not used because its cost (45) is greater than the variance times the current FD (40).

```
(config-router)#  
variance 2
```

- Router E chooses router C to get to network Z because FD = 20.
- With a variance of 2, router E chooses router B to get to network Z ($20 + 10 = 30 < [2 * (FD) = 40]$).
- Router D is not used to get to network Z ($45 > 40$).

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-10
0145_137

In the figure, the variance is 2, and the range of the metric values, which are the FDs for router E to locate network Z, is 20 through 45. This range of values determines 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 of the alternate path is within the variance. Load balancing can use only feasible paths, and the routing table includes only these paths. The two feasibility conditions are:

- Local best metric (current FD) is greater than the best metric (AD) learned from the next router. This condition exists if the next router in the path is closer to the destination than the current router. This approach prevents routing loops.
- Variance times the local best metric (current FD) is greater than the metric (FD) through the next router. This condition is true if the metric of the alternate path is within the variance.

If the path meets both of these conditions, the route is feasible and can be added to the routing table.

Note	Advertised distance (AD) is the metric that a neighbor uses to reach a given destination network. The AD is advertised as part of the EIGRP update for a given network. A router receiving the update adds its cost to reach that neighbor to the AD. The sum of these values provides the feasible distance (FD) to reach that destination network through that neighbor router.
-------------	---

In the figure, there are three paths to a given destination, and the metrics for these paths are:

- Path 1: 30 (top path)
- Path 2: 20 (middle path)
- Path 3: 45 (bottom path)

By default, the router places only path 2 in the routing table because it is the least-cost path. With EIGRP, you can use the **variance** command to instruct the router to route traffic to paths 2 and 3 in addition to path 1. Traffic is routed to any link that has a metric less than the best-path metric multiplied by the variance. To load balance over paths 1 and 2, use variance 2, because $20 * 2 = 40$, which is greater than the metric through path 1. Similarly, to also add path 3, you would issue the **variance 3** command under the **router eigrp** command process in configuration mode.

In this example, router E uses router C as the successor because it has the lowest FD (20). With the **variance** command applied to router E, the path through router B meets the criteria for load balancing. In this case, the FD through router B is less than twice the FD for the successor (router C). Router D is not considered for load balancing because the FD through router D is greater than twice the FD for the successor (router C).

EIGRP Bandwidth Utilization

This topic explains how to configure EIGRP to properly utilize the limited amount of bandwidth across a WAN link. Examples are provided to demonstrate different techniques to achieve proper bandwidth utilization.

Configuring WAN Links

Cisco.com

- **EIGRP supports different WAN links:**
 - Point-to-point links
 - NBMA
 - Multipoint links
 - Point-to-point links
- **EIGRP configurations can address bandwidth utilization over an interface:**
 - **EIGRP uses 50% of bandwidth by default**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-11

EIGRP operates efficiently in WAN environments. It is scalable on both point-to-point links and nonbroadcast multiaccess (NBMA) links.

Because of the inherent differences in the operational characteristics of the WAN links listed in the figure, the default configuration parameters for all WAN links may not be the best option. A solid understanding of EIGRP operation, coupled with knowledge of available link speeds, can yield an efficient, reliable, and scalable router configuration.

By default, EIGRP uses up to 50 percent of the bandwidth of an interface or subinterface, which is set with the **bandwidth** parameter. This percentage can be changed on a per-interface basis by using the **ip bandwidth-percent eigrp** interface configuration command. In this command, *nnn* is the percentage of the configured bandwidth that EIGRP can use. This percentage can be greater than 100. This capability is useful if the bandwidth is configured artificially low for routing-policy reasons.

Bandwidth Utilization over WAN Interfaces

Cisco.com

- **Bandwidth utilization over point-to-point subinterfaces using Frame Relay:**
 - Treats bandwidth as T1 by default
 - Best practice is to manually configure bandwidth as the CIR of the PVC
- **Bandwidth utilization over multipoint Frame Relay, ATM, SMDS, and ISDN PRI:**
 - EIGRP uses the bandwidth on the main interface divided by the number of neighbors on that interface to get the bandwidth information per neighbor.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-12

Cisco IOS software assumes that point-to-point Frame Relay subinterfaces (like all serial interfaces) operate at full T1 link speed. In many implementations, only fractional T1 speeds are available. When configuring these interfaces, set the bandwidth to match the contracted CIR on a per-subinterface basis.

When you are configuring multipoint interfaces, especially for Frame Relay (but also for ATM, SMDS, and ISDN PRI), it is important to understand that all neighbors share the bandwidth equally. EIGRP configuration should reflect the correct percentage of the actual available bandwidth on the line.

Bandwidth Utilization over WAN Interfaces (Cont.)

Cisco.com

- **Each PVC can have a different CIR, creating an EIGRP packet pacing problem.**
- **Multipoint interfaces:**
 - Convert to point-to-point configuration or manually configure bandwidth by multiplying the lowest CIR by the number of PVCs.

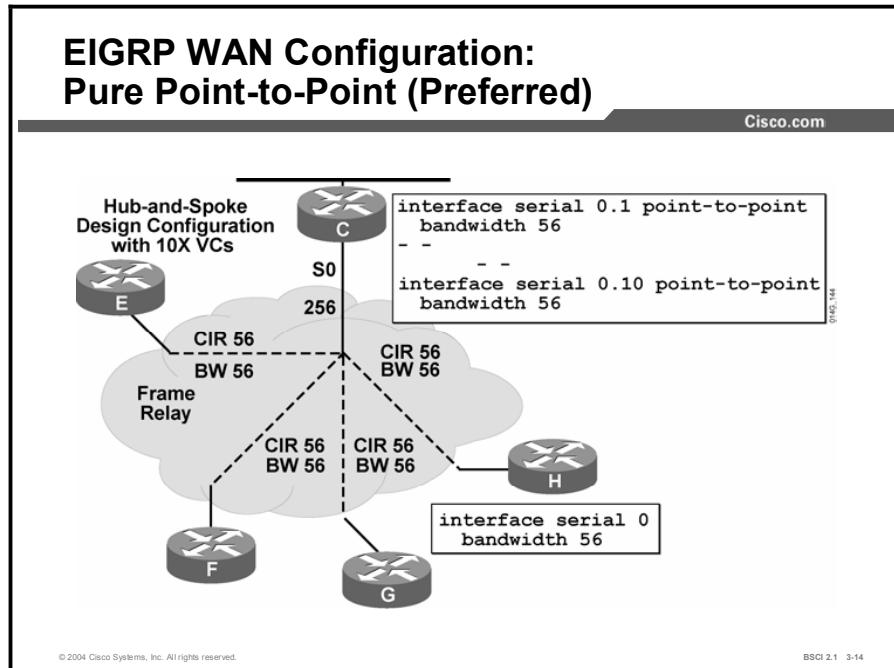
© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-13

Each installation has a unique topology and requires a unique configuration. Differing CIR values often require a hybrid configuration that blends the characteristics of point-to-point circuits with multipoint circuits. When you configure multipoint interfaces, configure the bandwidth to represent the minimum CIR multiplied by the number of circuits.

This approach may not use all of the higher-speed circuits, but it ensures that the circuits with the lowest CIR are not overdriven. If the topology has a small number of very low-speed circuits, these interfaces are typically defined as point-to-point so that their bandwidth can be set to match the provisioned CIR.

Example



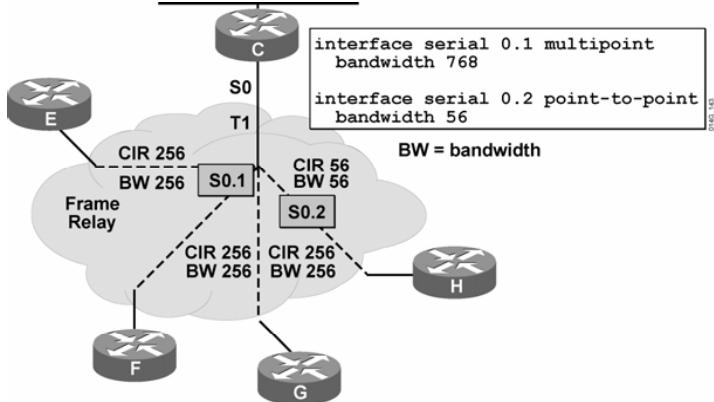
The figure illustrates a common hub-and-spoke design configuration topology with ten virtual circuits to the ten remote sites (only four of the ten remote sites are shown in the slide).

The circuits are provisioned as 56-kbps links. Point-to-point topology is used, and each subinterface is configured for 56-kbps bandwidth, matching its CIR. However, if the hub tries to communicate to all remote sites at the same time, the bandwidth that is required exceeds the available link speed of 256 kbps for the hub: 10 times the CIR of 56 kbps equals 560 kbps. If this problem occurs too often, higher bandwidth is needed at the hub side to support network operation.

The EIGRP default use is 50 percent of the configured bandwidth on the circuit. When you use a point-to-point subinterface configuration and manually configure bandwidth per subinterface as 56 kbps, each remote site can use up 28 kbps (50 percent of 56 kbps) to transmit EIGRP updates. When you use a point-to-point subinterface model, if a single remote site changes requirements because it needs more bandwidth or if EIGRP routing traffic is too heavy, the **ip eigrp bandwidth-percent** command can adjust the percentage of bandwidth that EIGRP uses on a per-subinterface basis.

EIGRP WAN Configuration: Hybrid Multipoint

Cisco.com



- Configure lowest CIR VC as point-to-point, specify BW = CIR
- Configure higher CIR VCs as multipoint, combine CIRs

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-15

This figure presents a hybrid solution. There is only one lower-speed circuit, and the other circuits are all provisioned to the same CIR.

The preferred configuration shows the low-speed circuit configured as point-to-point in an attempt to match the bandwidth with the CIR value. The remaining circuits are designated as multipoint, and their CIRs are added together to form the bandwidth for the interface. In multipoint interfaces, the bandwidth is shared equally among all circuits. Combining three CIRs of 256 kbps and then dividing their sum of 768 by 3 again matches the bandwidth allocation to the link capacity.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- EIGRP performs automatic network-boundary summarization, but administrators can disable automatic summarization and perform manual route summarization on an interface-by-interface basis.
- EIGRP performs equal-cost load balancing by default for up to four paths, but the limit is to a maximum of six paths.
- EIGRP can also perform unequal-cost load balancing using the variance command.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-16

Summary (Cont.)

Cisco.com

- Administrators can configure EIGRP to use less bandwidth on multipoint slow-speed links. Other routing protocols use up to 100 percent of the bandwidth for updates.
- By default, EIGRP uses only 50 percent of the bandwidth available for update traffic.
- The EIGRP bandwidth percentage can be changed on an interface or subinterface basis depending on network design and bandwidth constraints.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-17

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) By default, how many equal-cost paths to the same destination network can EIGRP place in the routing table?
- A) one
 - B) two
 - C) four
 - D) six
- Q2) Between headquarters and remote site A, there are two dedicated serial PPP connections, one at 64 kbps and the other at 128 kbps. What is the appropriate variance to allow for unequal-cost load balancing across these links?
- A) 1
 - B) 2
 - C) 3
 - D) 4
- Q3) What is the default bandwidth percentage that EIGRP will use on WAN links?
- A) 25 percent
 - B) 50 percent
 - C) 75 percent
 - D) 100 percent

Quiz Answer Key

Q1) C

Relates to: Understanding EIGRP Load Balancing

Q2) B

Relates to: Load Balancing Across Unequal-Cost Paths Using Variance

Q3) B

Relates to: EIGRP Bandwidth Utilization

EIGRP in a Scalable Network

Overview

EIGRP is a scalable routing protocol that ensures that as a network grows larger, it operates efficiently and adjusts rapidly to changes. This lesson describes practical EIGRP-specific design and configuration techniques to implement an effective scalable network.

Relevance

Network administrators benefit from understanding how to configure EIGRP to prevent common routing problems that hinder network scalability. For example, you can configure route summarization and implement EIGRP stub routers to limit the EIGRP query range, which enables the increased scalability of EIGRP internetworks with fewer complications.

Objectives

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

- Explain how EIGRP reacts to a query
- Describe how EIGRP query and reply functions behave on large internetworks
- Use route summarization to limit the EIGRP query range
- Limit the EIGRP query range using EIGRP stub areas
- List the EIGRP scalability rules

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **How EIGRP Responds to a Query**
- **Scalability Issues and Solutions**
- **Limiting the EIGRP Query Range with Route Summarization**
- **Limiting the EIGRP Query Range Using the Stub Option**
- **Scalability Rules for Implementing EIGRP**
- **Summary**
- **Quiz**

How EIGRP Responds to a Query

This topic describes how EIGRP routers respond to queries. This topic also examines an EIGRP routing condition called *stuck in active* (SIA).

EIGRP Query Process

Cisco.com

- **Queries are sent when a route is lost and no feasible successor is available.**
- **The lost route is now in active state.**
- **Queries are sent to all neighboring routers on all interfaces except the interface to the successor.**
- **If the neighbors do not have the lost-route information, queries are sent to their neighbors.**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-4

As an advanced distance vector protocol, EIGRP relies on neighboring routers to provide routing information. If a route is lost and no feasible successor is available, EIGRP needs to converge rapidly.

For fast convergence, EIGRP actively queries its neighboring routers for the lost route. The router seeks an alternate path to the destination, a condition known as going active on a route. The router queries its neighboring routers to determine whether they can provide an alternate path. If any of the queried routers have an alternate path, they provide the path in a reply packet. If not, these routers query each of their neighboring routers for an alternate path.

The queries then propagate through the network. If a router has an alternate route, it answers the query and does not propagate it further. The action of answering the query stops the query from spreading through that branch of the network; however, the query can still spread through other portions of the network as other routers attempt to find alternate pathways, which may not exist.

EIGRP Query Process SIA

Cisco.com

- **The router has to get all the replies from the neighbors with an outstanding query before the router calculates the successor information.**
- **If any neighbor fails to reply to the query within three minutes by default, the route is SIA, and the router resets the neighbor that fails to reply.**
- **A solution for SIA is to limit the query range, also known as query scoping.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-8

EIGRP uses a reliable multicast approach to search for an alternate to a lost route; therefore, it is imperative that EIGRP receive a reply for each query it generates in the network.

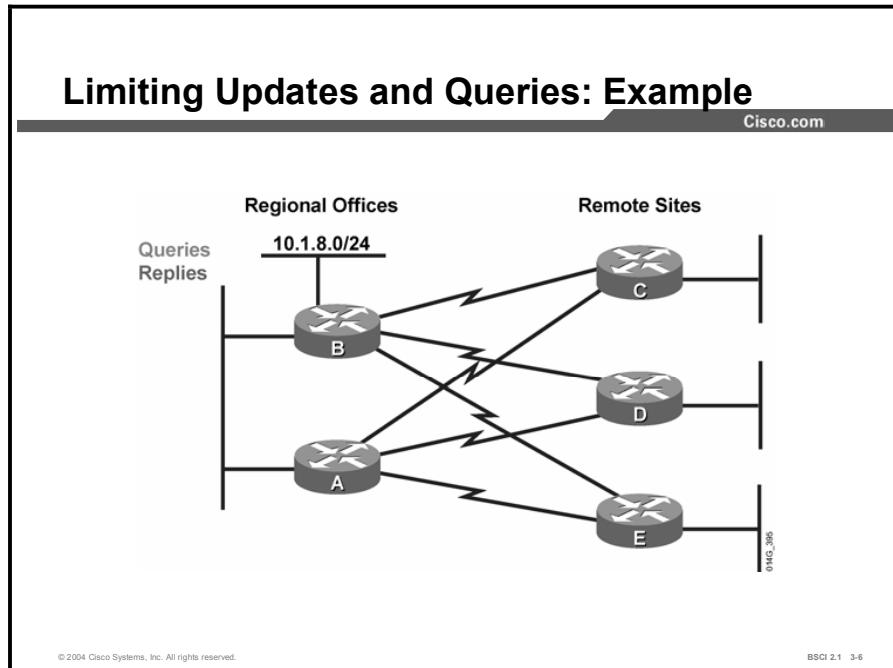
Once a route goes active and the query sequence is initiated, a route comes out of the active state only when it receives a reply for every generated query. If any neighboring router fails to reply to a query within three minutes, the route stays active at the querying router and resets the neighbor relationship to the neighbor that fails to reply. This setting causes the router to go active on all routes known through the lost neighbor. The router readvertises all routes that it knows about to the lost neighbor. This condition is SIA.

One way to help avoid the SIA condition is to limit the scope of query propagation through the network. Keeping the query packets close to the source reduces the chance that an isolated failure in another part of the network will restrict the convergence (query and reply) process.

The use of multiple EIGRP autonomous systems bounds the query range and can decrease the chances of an SIA route within the autonomous system. However, if a query reaches the edge of the autonomous system, where routes are redistributed into another autonomous system, the original query is answered but a new query is initiated in the other autonomous system. Therefore, the query process is not limited.

Another misconception of autonomous system boundaries is that implementation of multiple autonomous systems protects one autonomous system from route flaps in another autonomous system. If routes are redistributed between autonomous systems, route transitions from one autonomous system are detected in the other autonomous systems.

Example



In most networks, the network designer configures dual links to remote routers to improve their uptime when reaching the remainder of the network. Though this situation is not necessarily desirable, traffic can go from the regional office to the remote office and back to the regional office as though this link were a valid alternate path.

The figure shows a sample network in which each dual-homed remote router has two valid paths to 10.1.8.0 from router A and router B. With this topology, once the query process starts, each path between the regional routers and the remote routers receives duplicate convergence traffic (queries and replies) because of the redundancy designed into the topology.

For example, if the 10.1.8.0/24 network goes down at router B, multiple queries and replies are sent between the regional routers (A and B) and the remote routers (C, D, and E) because of the redundant topology. This increase in traffic significantly complicates the convergence process on the network.

In the sample network with only two regional and three remote routers, the problem may not be highly significant. In a network with hundreds of remote offices, the problem can be severe.

The following text provides a detailed explanation of the query process for the 10.1.8.0/24 subnet. In the example for network 10.1.8.0/24, router B advertises 10.1.8.0/24 to all other routers. The best pathway for router A to reach 10.1.8.0/24 is over the Ethernet link to router B. The remote routers (C, D, and E) use the serial link to B as their preferred pathway to reach 10.1.8.0/24 but still learn about an alternate pathway through router A. For this example, assume that the EIGRP metric cost of Ethernet is 1000 and the metric cost of a serial link is 100,000.

The table shows the values contained, for network 10.1.8.0/24, in the IP EIGRP topology table for routers A, C, D, and E.

Routers C, D, and E IP EIGRP Table

	FD	AD
Router B	101,000	1,000
Router A	102,000	2,000

Router A IP EIGRP Table

	FD	AD
Router B	2,000	1,000
Router C	201,000	101,000
Router D	201,000	101,000
Router E	201,000	101,000

Note that routers C, D, and E determine that router A is a feasible successor for network 10.1.8.0/24 because their AD is 2,000 through router A, which is less than the FD through router B. Also, note that router A does not have a feasible successor because all pathways through the remote routers have an AD larger than the FD through router B.

When router B loses the pathway to network 10.1.8.0/24, it queries all four of its neighbors. As a result of DUAL, when the remote sites receive this query, they automatically use the pathway through router A and respond to router B with their supposedly good pathway through router A. They also remove the bad pathway through router B in their topology table.

Router B now has responses to three of its four queries, but it must wait until router A responds as well.

When router A received the query from router B for network 10.1.8.0/24, router A did not have a feasible successor but knew that a pathway existed through each remote site to reach 10.1.8.0/24. Router A creates a query and sends it to routers C, D, and E.

Routers C, D, and E receive the query from router A and check their topology tables for alternate pathways. However, none of these routers currently have another pathway because router B just informed these routers that it did not have a pathway to this network. Because the remote routers do not have an answer to the query from router A, routers C, D, and E create a query and send it to all neighbors except for the neighbor (interface) that these routers received the original query from. In this case, the remote routers send the query to router B.

Router B learns from these queries that none of the remote routers have a pathway to network 10.1.8.0/24, but it cannot respond that it does not know of a pathway because router B is waiting for router A to reply to a query. Router A is waiting for either router C, D, or E to reply to its query, and these remote sites are waiting for router B to reply to their queries. Router B reaches the SIA state for network 10.1.8.0/24 in three minutes by default. Since router B sent out the first query, its SIA timer expires first and router B resets its neighbor relationship with router A. Once the neighbor relationship goes down, router B can respond to routers C, D, and

E immediately, saying that router B does not have a pathway to 10.1.8.0/24. Routers C, D, and E can then respond to router A that they do not have a pathway.

After the EIGRP neighbor relationship between routers A and B has been reestablished (just after resetting the adjacency), router B, which no longer has a pathway to 10.1.8.0/24, does not pass the 10.1.8.0 network to router A. Router A learned that the remote sites do not have a pathway to 10.1.8.0/24, and the new relationship with router B does not include a pathway to 10.1.8.0/24, so router A removes the 10.1.8.0 network from its IP EIGRP topology table.

Limiting Updates and Queries: Reality

Cisco.com

- **Remote routers are fully involved in convergence.**
- **Convergence is complicated by the lack of information hiding.**
- **Traffic from one regional office to other regional offices is usually not intended to travel through the remote offices.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-16

The design of this sample network is sound, but because of the EIGRP query process, the remote routers become too involved in the convergence process. In addition, the remote routers have too much information in their EIGRP topology table and routing table.

If the remote sites are not acting as transit sites between the regional sites, the regional routers can be configured to announce only a default route to the remote routers; the remote routers can be configured to announce only their directly connected stub network to the regional routers to reduce the complexity and the EIGRP topology table and routing table size.

Scalability Issues and Solutions

This topic describes how EIGRP query and reply functions behave on large internetworks.

Factors That Influence EIGRP Scalability

Cisco.com

- **EIGRP is not plug and play for large networks.**
- **EIGRP query propagation can be extensive.**
- **The quantity of routing information exchanged between peers without proper route summarization can be excessive.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-17

Some of the factors that affect network scalability are, as follows:

- **Amount of information exchanged between neighbors:** If more information is passed than necessary for routing to function correctly, EIGRP has to work harder at neighbor startup and to react to changes in the network.
- **Number of routers:** When a change occurs in the network, EIGRP resource consumption directly relates to the number of routers involved in the change.
- **Depth of the topology:** Depth of topology becomes an issue when information propagates through many hops (depth) for convergence. A multinational network without route summarization is an example of this type of condition. A three-tiered network design is highly recommended for all IP routing environments. There should never be more than seven hops between any two routing devices on an internetwork. The delay of propagation for changes and queries across these multiple hops slows down convergence of the network for lost routes.
- **Number of alternate paths through the network:** A network should provide alternate paths to avoid single points of failure. However, too much complexity (alternate paths) can also create EIGRP convergence problems because the EIGRP routing process, using queries, needs to explore all possible pathways for lost routes. This complexity creates an ideal condition for a router to become SIA as it awaits a response to queries that are being propagated through these many alternate paths.

Limiting the EIGRP Query Range with Route Summarization

This topic examines how to limit the EIGRP query range using the **ip eigrp summarization** command. This topic also discusses the effectiveness of this method.

Limiting Size and Scope of Updates and Queries

Cisco.com

- **Evaluate routing requirements:**
 - What routes are needed where?
- **Once needs are determined:**
 - Use summary address
 - Use EIGRP stub command

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-18

The network manager determines the information needed to properly route user traffic to the appropriate destination.

Trade-offs must be made to determine how much information is needed by the remote routers to achieve the desired level of path selection. When you achieve maximum stability and scalability, the remote routers can use a default route to reach the core. If some specific networks need knowledge of more routes to ensure optimum path selection, you must make a business decision about whether the propagation of additional routing information offers more benefits than using the additional bandwidth to achieve this goal.

In a properly designed network, each remote site has redundant WAN links to separate distribution sites. If both distribution sites pass a default route to the remote site, the remote site load-balances to all networks behind the distribution sites. This process maximizes bandwidth utilization and allows the remote router to use less CPU and memory, which means that a smaller and less expensive remote router can be used at that site.

If you allow the remote site to see all routes, the router can select the path on the distribution router that is best to reach a given network. But, depending on the number of routes in the internetwork and the amount of bandwidth connecting the remote site to the distribution sites, this approach can mean that higher-bandwidth links or large routers are needed to handle the additional overhead.

Once you determine the minimum routing requirements, you can make EIGRP more scalable. Two of the best options are the following:

- Configure route summarization using the **ip summary-address eigrp** command on the outbound interfaces of the appropriate routers.
- Configure remote routers as stub EIGRP routers.

Summarizing routes limits the scope of the queries by limiting the knowledge a router has of the subnets of a network. If a subnet goes down, queries go only as far as the routers that had knowledge of the subnet.

A remote router configured with an EIGRP stub informs upstream distribution routers not to pass queries to this EIGRP stub router, because it has no downstream EIGRP neighbors and thus does not have alternate pathways for lost routes. Therefore, upstream routers do not query EIGRP stub routers for lost routes.

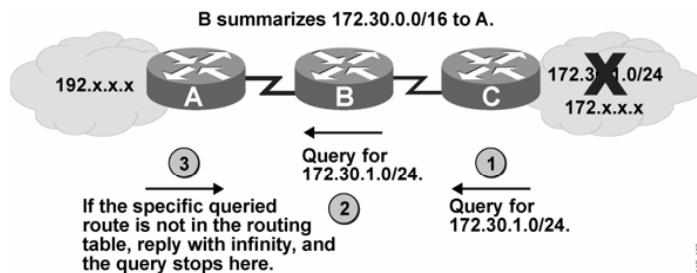
Other methods to limit query range include route filtering or interface packet filtering. For example, if a router filters EIGRP routing updates, blocking specific networks, when the router receives a query about those filtered (blocked) networks, the router indicates that the network is unreachable. The router does not extend the query any further.

EIGRP Query Range: Summarization

Cisco.com

Summarization point:

- Auto or manual summarization is one of the best ways to bound queries.
- It requires a good address allocation scheme.



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-19

One of the best ways to limit the EIGRP query range is to use route summarization.

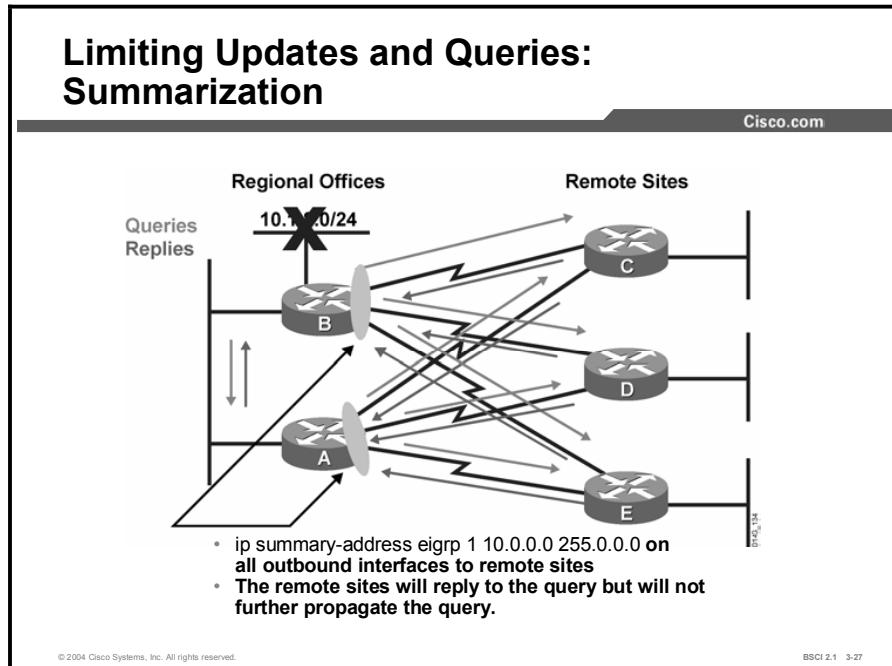
In the figure, router B sends a summary route of 172.30.0.0/16 to router A. When network 172.30.1.0/24 goes down, router A receives a query from router B about that network. Because router A has received only a summary route, that specific network is not in the routing table. Router A replies to the query with a “network 172.30.1.0/24 unreachable” message and does not extend the query any further.

The query range is not a common cause of SIA routes. The most common reasons for SIA routes are the following:

- The router is too busy to answer the query, generally as a result of high CPU usage; the router has memory problems and cannot allocate the memory to process the query or build the reply packet.
- The link between the two routers is not good; therefore, some packets are lost between the routers. The router receives enough packets to maintain the neighbor relationship; however, the router does not receive all queries or replies.
- A failure causes traffic on a link to flow in only one direction—a unidirectional link.

These problems can be beyond the control of the network administrator. However, summarization allows the size of the routing table to be minimized which means less CPU usage to manage it and less bandwidth to transmit the information. Summarization reduces the chance of networks becoming SIA. When you are limiting the query range with summarization, the number of routers that see each query is reduced so that the chances of a query encountering one of these issues is also reduced.

Example



In this example, route summarization prevents EIGRP queries for the lost 10.1.8.0/24 networks from being propagated beyond the remote sites, preventing router A and B from becoming SIA while waiting for the query process to receive all the replies.

With the **ip summary-address eigrp** commands configured on the outbound interfaces of routers A and B, routers A and B advertise the 10.0.0.0/8 summary route to the remote routers C, D, and E.

The 10.1.8.0/24 network is not advertised to the remote routers. Therefore, the remote routers (C, D, and E) do not extend the queries about the 10.1.8.0/24 network back to the regional routers (A and B). This approach reduces the convergence traffic (queries and replies) caused by the redundant topology.

LIMITING UPDATES AND QUERIES: SUMMARY

Cisco.com

Convergence is simplified by adding the summary address statements:

- Remote routers extend the query about a network only if it has an exact match in the routing table.
- In the case of the previous example, routers C, D, and E know about 10.0.0.0/8 only because of the EIGRP summary address statement.
- Routers A and B query router C and the other remote routers about an alternate route to 10.1.8.0/24. Since router C never had an entry for that network, it can immediately respond with destination unreachable without extending the query any further.

Query From	Route State	Action
Any neighbor	Not known before query	Reply that the destination is unreachable

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-28

Performing route summarization at key points simplifies convergence; remote routers reply that a network is not reachable and do not extend the query any further if the queried network does not have an exact match in the routing table.

In the previous example, the summarization command on the serial interfaces for routers A and B instructs EIGRP to advertise 10.0.0.0/8 and suppress the more specific routes, such as 10.1.8.0/24, from being announced to routers C, D, and E.

When routers A and B send the query for 10.1.8.0/24 to routers C, D, and E, these routers immediately reply to routers A and B that the destination is unreachable. Routers C, D, and E only have a summary entry for 10.0.0.0/8, so they do not extend the query for the 10.1.8.0/24 subnet any further.

Limiting the EIGRP Query Range Using the Stub Option

This topic describes an efficient way to limit the EIGRP query range using the EIGRP stub option for remote routers.

Configuring EIGRP Stub

Cisco.com

```
Router(config-router)#  
eigrp stub [receive only|connected|static|summary]
```

- The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies remote router (spoke) configuration.
- Stub routing is commonly used in a hub-and-spoke topology.
- A stub router sends a special peer information packet to all neighboring routers to report its status as a stub router.
- Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes.

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 3-30

When using the EIGRP stub routing feature, only the remote routers must be configured as stubs. Using the EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration.

The EIGRP stub feature was first introduced in Cisco IOS Software Release 12.0(7)T. It has the following characteristics:

- Hub-and-spoke network topology commonly uses stub routing. In this topology, the remote router forwards all traffic that is not local to a hub router. The remote router does not need to retain a complete routing table. Generally, the hub router needs to send only a default route to the remote routers.
- A stub router sends a special peer information packet to all neighboring routers to report its status as a stub router. A neighbor that receives a packet informing it of the stub status does not query the stub router for any routes. Therefore, a router that has a stub peer does not query that peer. Only the remote router is configured as a stub. The stub routing feature does not prevent routes from being advertised to the remote router. In a hub-and-spoke topology, having a full route table on the remote router serves no functional purpose because the path to the corporate network and the Internet is always through the hub router. Additionally, having a full route table at the spoke router increases the amount of memory required. Route summarization and route filtering can be used to conserve bandwidth and memory requirements on the spoke routers.

A router configured as a stub with the **eigrp stub** command shares information about connected and summary routes with all neighboring routers by default.

The following four optional keywords can be used with the **eigrp stub** command to modify this behavior:

- **receive-only:** The **receive-only** keyword restricts the router from sharing any of its routes with any other router within an EIGRP autonomous system. This keyword does not permit any other option to be specified, because it prevents any type of route from being sent. The three other optional keywords (**connected**, **static**, and **summary**) cannot be used with the **receive-only** keyword. Use this option if there is a single interface on the router.
- **connected:** The **connected** keyword permits the EIGRP stub-routing feature to send connected routes. If a network statement does not cover connected routes, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default and this is the most widely practical stub option.
- **static:** The **static** keyword permits the EIGRP stub-routing feature to send static routes. Redistributing static routes with the **redistribute static** command is still necessary.
- **summary:** The **summary** keyword permits the EIGRP stub-routing feature to send summary routes. Summary routes can be created manually with the **summary-address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **eigrp stub** command can be modified with several options that can be used in any combination, with the exception of the **receive-only** keyword. If one of these keywords, except **receive-only**, is used individually with the **eigrp stub** command, **connected** and **summary** routes are not sent automatically.

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
router eigrp 1
network 10.0.0.0
eigrp stub
```

In the following example, the **eigrp stub receive-only** command is used to configure the router as a stub. Connected, summary, or static routes are not sent.

```
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub receive-only
```

In the following example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
router eigrp 1
network 10.0.0.0
eigrp stub connected static
```

The EIGRP stub-routing feature does not automatically enable route summarization on the hub router. In most cases, the network administrator should configure route summarization on the hub routers.

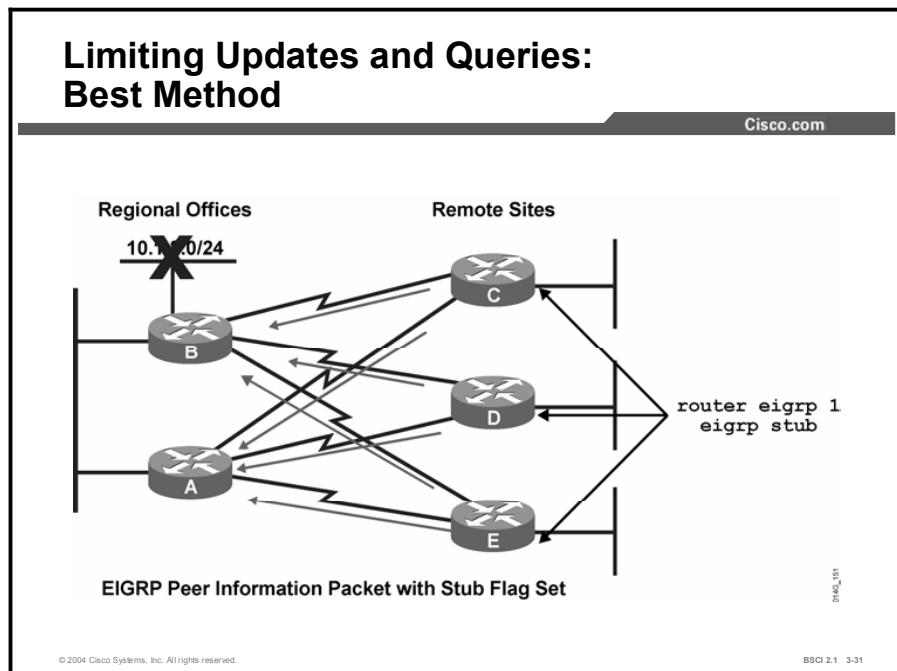
If a true stub network is required, the hub router can be configured to send a default route to the spoke routers. This approach is the most simple and conserves the most bandwidth and memory on the spoke routers.

Note Although EIGRP is a classless routing protocol, it has classful behavior by default, such as having autosummarization on by default.

When you configure the hub router to send a default route to the remote router, use the **ip classless** command on the remote router. By default, the **ip classless** command is enabled in all Cisco IOS images that support the EIGRP stub-routing feature.

Without the stub feature, EIGRP sends a query to the spoke routers if a route is lost somewhere in the corporate network. If there is a communication problem over the WAN link between the hub router and the spoke router, an EIGRP SIA condition can occur and cause instability elsewhere in the network. The EIGRP stub-routing feature allows a network administrator to prevent sending queries to the spoke router under any condition. It is highly recommended that you use both EIGRP route summarization and EIGRP stub features to provide the best scalability.

Example



Using the EIGRP stub feature at the remote sites allows the hub (regional) sites to immediately answer queries without propagating the queries to the remote sites, saving CPU cycles and bandwidth, and lessening convergence time even when the remote sites are dual-homed to two or more hub (regional) sites.

Traffic from a hub router should not use a remote router as a transit path. A typical connection from a hub router to a remote router has significantly less bandwidth than a connection at the network core. Attempting to use a remote router with a limited-bandwidth connection, such as a transit path, typically produces excessive congestion to the remote router. The EIGRP stub-routing feature can prevent this problem by restricting the remote router from advertising the regional routes back to hub routers. Routes recognized by the remote router from hub router A are not advertised to hub router B. Since the remote router does not advertise the regional routes back to the hub routers, the hub routers do not use the remote routers as a transit for traffic destined for the regional networks.

The EIGRP stub-routing feature can help to provide significant network stability. In the event of network instability, this feature prevents EIGRP queries from being sent over limited-bandwidth links to nontransit routers. Instead, hub routers connected to the stub router answer the query on behalf of the stub router. This feature reduces the chance of further network instability due to congested or problematic WAN links.

The EIGRP stub-routing feature simplifies the configuration and maintenance of hub-and-spoke networks. When stub routing is enabled in dual-homed remote configurations, you do not have to configure filtering on remote routers to prevent them from appearing as transit paths to the hub routers.

Caution EIGRP stub routing should be used on stub routers only. A stub router is defined as a router connected to the network core or hub layer through which core transit traffic should not flow. A stub router should have hub routers only for EIGRP neighbors. Ignoring this restriction causes undesirable behavior.

Scalability Rules for Implementing EIGRP

This topic describes implementation rules for EIGRP.

Nonscalable Network Addressing

Cisco.com

- Poor addressing scheme limiting summarization
- Queries not bounded
- Default bandwidth statements for WAN and Frame Relay

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 3-32

EIGRP has many features that allow the creation of a range of large internetworks. The infrastructure for any large network rests on good, solid design principles.

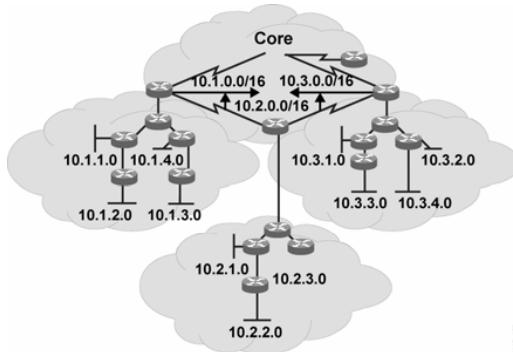
Regardless of the selected advanced routing protocol, address allocation is critical to any design effort because route summarization requires logical blocks of addresses.

Adequate bandwidth is required on WAN links, particularly for hub-and-spoke topologies. There should be enough bandwidth to prevent necessary router overhead traffic from interfering with normal user-generated traffic. If reliable EIGRP packets are lost due to competition for bandwidth, a lack of convergence can be a far greater problem than the application delays experienced by some users. If the EIGRP routing process does not converge, then networks may become unreachable to all the users.

The figure illustrates a topology where addresses, subnets, are either randomly assigned or are assigned by historical requirements. Each cloud contains multiple subnets from different major networks. The number of routes injected into the core is greater than necessary because route summarization is not possible. In addition, because of the random assignment of addresses, query traffic cannot be localized to any portion of the network. The inability to localize query traffic increases convergence time.

Scalable Network Addressing

Cisco.com



- Good addressing scheme promoting summarization
- Queries bounded by using summarization and stub feature
- Appropriate bandwidth statement for WAN and Frame Relay

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 3-33

The figure illustrates a well-designed network. Subnet addresses forming individual major networks are localized with each of the clouds. This design allows summary routes to be created and injected into the core. Another benefit of this design is that the summary routes act as a boundary for the queries generated by a topology change.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- EIGRP is not a plug-and-play feature for large networks. Like other major routing protocols, it must be designed and configured properly.
- Limiting the amount of routing information a given router needs to deal with is a major factor in eliminating scaling problems such as SIA.
- EIGRP offers a number of choices for preventing issues like SIA, such as EIGRP route summarization and EIGRP stub router configuration.
- When using EIGRP route summarization, the more specific subnets are suppressed, and summarized routes are advertised to remote sites.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-34

Summary (Cont.)

Cisco.com

- When queried by distribution sites for the more specific subnets, the remote sites can immediately respond with destination unreachable.
- Using the **eigrp stub router** command, remote sites inform upstream sites that they are stub routers and should not be queried for lost routes. The upstream routers answer all queries for the remote sites.
- Combining three approaches: a default route, proper route summarization, and using stub networks, is an effective solution for scaling EIGRP networks to large sizes.
- For scaling EIGRP, the proper resources such as bandwidth, CPU cycles, and memory have to be available. The network should have good IP address allocation for summarization and a hierarchical design.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 3-35

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) When a router gets a query from a neighboring router that is not a successor for the network listed in the query, and that network is in a passive state on this router, what does the router do?
- A) The router replies that the destination is unreachable.
 - B) The router attempts to find a new successor; if successful, it replies with new information. If the router is not successful, it marks the destination unreachable and queries all neighboring routers except the previous successor.
 - C) The router replies with the current successor information.
 - D) The router marks the destination unreachable and queries all neighboring routers except the previous successor.
- Q2) Which three factors impact network scalability? (Choose three.)
- A) number of alternate paths through the network
 - B) amount of information exchanged between neighbors
 - C) autonomous systems boundaries
 - D) depth of the topology
- Q3) Which example demonstrates the proper use of the EIGRP route summarization command for network 10.1.0.0/16 in AS 100?
- A) outbound interface command: **ip summary-address 10.1.0.0 255.255.0.0**
 - B) router EIGRP command: **summary-address 10.1.0.0 255.255.0.0**
 - C) outbound interface command: **ip summary-address eigrp 100 10.1.0.0 255.255.0.0**
 - D) inbound interface command: **ip summary-address 10.1.0.0 255.255.0.0**
- Q4) Which three statements are true for implementing EIGRP stub routers? (Choose three.)
- A) Stub routing is commonly used on hub-and-spoke design configuration networks.
 - B) The EIGRP stub feature should be configured only on remote spoke routers.
 - C) EIGRP stub routers can and should be used at a transit point to other parts of the network and other autonomous systems.
 - D) Queries are not propagated to EIGRP stub routers. EIGRP updates are sent to stub routers, or a default route is passed.

Quiz Answer Key

Q1) C

Relates to: How EIGRP Responds to a Query

Q2) A, B, D

Relates to: Scalability Issues and Solutions

Q3) C

Relates to: Limiting the EIGRP Query Range with Route Summarization

Q4) A, B, D

Relates to: Limiting the EIGRP Query Range Using the Stub Option

Lesson Assessments

Overview

Use this assessment 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:

- Quiz 3-1: EIGRP Overview
- Quiz 3-2: EIGRP Operations
- Quiz 3-3: EIGRP DUAL
- Quiz 3-4: Configuring and Verifying EIGRP
- Quiz 3-5: Advanced EIGRP Configuration Options
- Quiz 3-6: EIGRP in a Scalable Network

Quiz 3-1: EIGRP Overview

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

Objectives

This assessment tests your knowledge of how to:

- Define the key features of EIGRP
- List the types of EIGRP databases
- Describe the EIGRP metric calculation

Quiz

Answer these questions:

- Q1) Which three characteristics are key features of EIGRP? (Choose three.)
 - A) rapid convergence
 - B) reduced bandwidth usage
 - C) support for multiple Layer 3 protocols
 - D) backward compatibility with RIP
- Q2) Which three features are benefits of EIGRP? (Choose three.)
 - A) use of SPF to achieve fast convergence
 - B) ease of configuration
 - C) support for VLSM
 - D) incremental updates
- Q3) Which two characteristics are features of EIGRP? (Choose two.)
 - A) support for load balancing across unequal-cost paths
 - B) manual summarization at any point on the internetwork
 - C) provision of highly structured area design requirements
- Q4) Which type of database is a listing of all EIGRP adjacencies?
 - A) EIGRP topology table
 - B) EIGRP neighbor table
 - C) IP routing table
- Q5) Which type of database contains a listing of all the best EIGRP routes to reach a destination?
 - A) EIGRP topology table
 - B) EIGRP neighbor table
 - C) IP routing table
- Q6) Which type of database contains a listing of all possible EIGRP routes to reach a destination?
 - A) EIGRP topology table
 - B) EIGRP neighbor table
 - C) IP routing table

Q7) Which five criteria can be considered by EIGRP to calculate the metric?
(Choose five.)

- A) MTU
- B) bandwidth
- C) cost
- D) delay
- E) loading
- F) hop count
- G) reliability

Q8) Which two criteria are used by EIGRP to calculate the metric by default?
(Choose two.)

- A) MTU
- B) bandwidth
- C) cost
- D) delay
- E) loading
- F) hop count
- G) reliability

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 3-2: EIGRP Operations

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

Objectives

This assessment tests your knowledge of how to:

- Describe EIGRP packets
- Explain EIGRP adjacent neighbors
- Define EIGRP reliability, transmission policy, and transport mechanism
- Describe initial route discovery
- Interpret debug output for EIGRP packets, EIGRP neighbors, and IP EIGRP

Quiz

Answer these questions:

- Q1) What is the function of an EIGRP ACK packet?
 - A) It establishes neighbor relationships.
 - B) It is responsible for sending routing advertisements.
 - C) It acknowledges a reliable packet.
 - D) It responds to a query.
 - E) It asks neighbors about routing information.
- Q2) What is the function of an EIGRP update packet?
 - A) It establishes neighbor relationships.
 - B) It is responsible for sending routing advertisements.
 - C) It acknowledges a reliable packet.
 - D) It responds to a query.
 - E) It asks neighbors about routing information.
- Q3) What is the function of an EIGRP reply packet?
 - A) It establishes neighbor relationships.
 - B) It is responsible for sending routing advertisements.
 - C) It acknowledges a reliable packet.
 - D) It responds to a query.
 - E) It asks neighbors about routing information.
- Q4) What is the function of an EIGRP query packet?
 - A) It establishes neighbor relationships.
 - B) It is responsible for sending routing advertisements.
 - C) It acknowledges a reliable packet.
 - D) It responds to a query.
 - E) It asks neighbors about routing information.

- Q5) What is the function of an EIGRP hello packet?
- A) It establishes neighbor relationships.
 - B) It is responsible for sending routing advertisements.
 - C) It acknowledges a reliable packet.
 - D) It responds to a query.
 - E) It asks neighbors about routing information.
- Q6) Which three requirements are necessary to establish an EIGRP adjacency? (Choose three.)
- A) K values do not need to match.
 - B) Neighbors must use the same autonomous system number.
 - C) Hello and hold timers do not need to match.
 - D) Primary address of the adjacent routers must be in the same subnet.
- Q7) Which two packets are not explicitly acknowledged? (Choose two.)
- A) ACK
 - B) hello
 - C) reply
 - D) update
- Q8) How many update packets can the EIGRP transport mechanism send before it must wait for an acknowledgment?
- A) 1
 - B) 7
 - C) 15
 - D) 16

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 3-3: EIGRP DUAL

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

Objectives

This assessment tests your knowledge of how to:

- Match a term used to describe EIGRP DUAL with the appropriate function.

Quiz

- Q1) Test your understanding of EIGRP by matching terms with statements. Write the letter of the statement in front of the term that the statement describes. A statement may describe several terms.

Term

- 1. successor
- 2. feasible successor
- 3. hello
- 4. topology table
- 5. IP
- 6. update
- 7. routing table
- 8. DUAL

Statement

- A) a network protocol that EIGRP supports
- B) a database that contains successor and feasible successor information
- C) a database that includes administrative distance
- D) a neighbor router that has the best path to a destination
- E) a neighbor router that has the best alternative path to a loop-free destination
- F) an algorithm used by EIGRP to ensure fast convergence
- G) a multicast packet used to discover neighbors
- H) a packet sent by EIGRP routers when a new neighbor is discovered and a change occurs

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 3-4: Configuring and Verifying EIGRP

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

Objectives

This assessment tests your knowledge of how to:

- Configure EIGRP
- Configure a default route using the **default-network** command
- Verify EIGRP using **show** commands

Quiz

Answer these questions:

- Q1) Which is true regarding the EIGRP autonomous system number?
- A) is an optional parameter that can be left blank
 - B) must be different on each router that wants to exchange EIGRP updates
 - C) must be the same on each router that wants to exchange EIGRP updates
 - D) is an IP address
- Q2) The correct wildcard mask to use in a **network** statement that allows updates to propagate only out interfaces that are part of subnet 10.1.0.0 is:
- A) **network 10.1.0.0 mask 255.255.0.0**
 - B) **network 10.1.0.0 mask 0.0.255.255**
 - C) **network 10.1.0.0 255.255.0.0**
 - D) **network 10.1.0.0 0.0.255.255**
- Q3) Which three are required when configuring the **ip default-network** command for EIGRP? (Choose three.)
- A) must be reachable by the router using this command
 - B) will set the gateway of last resort to 0.0.0.0 on the router issuing this command
 - C) must be advertised to other neighbors as an EIGRP route
 - D) will be flagged by other EIGRP routers as a candidate default route
- Q4) What does the passive state in the EIGRP topology table signify?
- A) There are outstanding queries for this network.
 - B) The network is unreachable.
 - C) The network is up and operational, and this state signifies normal conditions.
 - D) A feasible successor has been selected.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 3-5: Advanced EIGRP Configuration Options

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

Objectives

This assessment tests your knowledge of how to:

- Describe and configure EIGRP manual route summarization
- Describe and configure load balancing across equal paths
- Describe and configure unequal-cost load balancing in EIGRP using the **variance** command
- Describe and configure EIGRP bandwidth utilization on WAN links

Quiz

Answer these questions:

- Q1) Which command is used to disable automatic network-boundary summarization, and where is it applied?
- A) **no boundary-summarization** at the interface level
 - B) **no auto-summary** under the routing process
 - C) **no auto-summary** at the interface level
 - D) **no boundary-summarization** under the routing process
- Q2) Which command is used for manual summarization of all the subnets for network 10.1.32.0/21 for EIGRP in autonomous system 101?
- A) **ip summary-address eigrp 101 10.1.32.0 255.255.248.0**
 - B) **ip eigrp 101 summary-address 10.1.32.0 255.255.240.0**
 - C) **ip summary-address eigrp 101 10.1.32.0 255.255.240.0**
 - D) **ip eigrp 101 summary-address 10.1.32.0 255.255.248.0**
- Q3) What is the default bandwidth percentage that EIGRP uses on a WAN link when transmitting EIGRP packets?
- A) 30 percent
 - B) 50 percent
 - C) 75 percent
 - D) 100 percent

Scoring

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

Quiz 3-6: EIGRP in a Scalable Network

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

Objectives

This assessment tests your knowledge of how to:

- Explain how EIGRP reacts to a query
- Describe how EIGRP query and reply functions behave on large internetworks
- Use route summarization to limit the EIGRP query range
- Limit the EIGRP query range using EIGRP stub areas
- List the EIGRP scalability rules

Quiz

Answer these questions:

- Q1) If a neighbor fails to reply to a query, the route is SIA. How long does the querying router wait to reset the neighbor that fails to reply?
- A) 15 seconds
 - B) 40 seconds
 - C) 1 minute
 - D) 3 minutes
- Q2) What are the two best ways to perform query scoping? (Choose two.)
- A) use EIGRP route summarization
 - B) adjust the EIGRP metric
 - C) configure the remote routers as EIGRP stub routers
 - D) use packet filtering to deny EIGRP queries from propagating to other EIGRP neighbors

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent or better.

Lesson Assessment Answer Key

Quiz 3-1: EIGRP Overview

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

Quiz 3-2: EIGRP Operations

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

Quiz 3-3: EIGRP DUAL

- Q1) 1-D, 2-E, 3-G, 4-B, 5-A, 6-H, 7-C, 8-F

Quiz 3-4: Configuring and Verifying EIGRP

- Q1) C
- Q2) D
- Q3) A, C, D
- Q4) C

Quiz 3-5: Advanced EIGRP Configuration Options

- Q1) B
- Q2) A
- Q3) B

Quiz 3-6: EIGRP in a Scalable Network

- Q1) D
- Q2) A, C

Module 4

Configuring OSPF

Overview

This module examines Open Shortest Path First (OSPF), which is one of the most commonly used interior gateway protocols in IP networking. OSPF is an open-standard protocol based primarily on RFC 2328. OSPF is a fairly complex protocol made up of several protocol handshakes, database advertisements, and packet types.

Configuration and verification of OSPF in a Cisco Systems router is a primary objective of this module. The lessons move from simple to more advanced configuration topics. Each of the important OSPF commands is explained and described in an example. All the important OSPF **show** commands are defined.

Module Objectives

Upon completing this module, you will be able to configure and verify OSPF in a Cisco router.

Module Objectives

Cisco.com

- **List the characteristics and features of OSPF**
- **Explain how OSPF operates in a single-area domain**
- **Configure and verify OSPF for a single-area design**
- **Identify the five types of OSPF packets and explain their role in the establishment of neighbor adjacencies**
- **Describe the types of link-state advertisements and accurately interpret an OSPF link-state database and routing table**
- **Configure OSPF route summarization for interarea and external routes**
- **Identify the specific OSPF area types and configure each area**
- **Configure an OSPF virtual link and verify its operation**

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- OSPF Protocol Overview
- OSPF Packet Types
- Configuring Basic OSPF
- OSPF Network Types
- Types of OSPF Routers and Link-State Advertisements
- OSPF Route Summarization Techniques
- OSPF Special Area Types
- OSPF Virtual Links
- Lesson Assessments

OSPF Protocol Overview

Overview

This lesson introduces each of the major components that make up the OSPF routing protocol. This lesson defines the major characteristics of the OSPF routing protocol and provides a brief definition of link-state routing protocols, link-state adjacencies, and shortest path first (SPF) calculations.

Relevance

OSPF is one of the most commonly used IP routing protocols in networking. It is an open standard used by both enterprise and service provider networks.

Objectives

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

- Describe the concept of link-state routing protocol
- Identify the purpose of OSPF areas
- Describe the concept of OSPF adjacencies
- Explain the OSPF SPF calculation

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- An understanding of IP subnetting, variable-length subnet masking (VLSM), and route summarization
- General knowledge of the Cisco IOS software user interface
- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

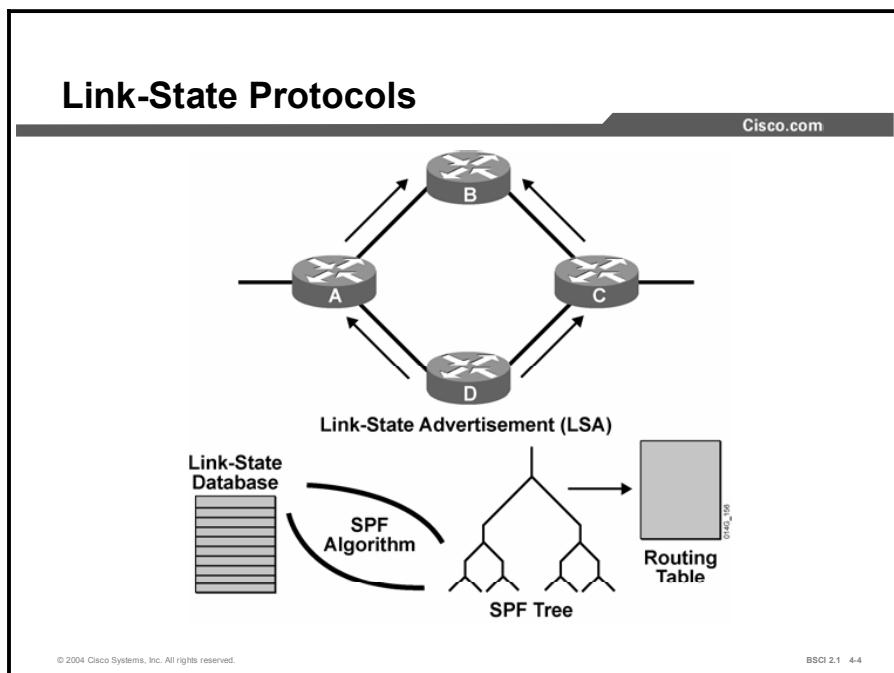
Outline

Cisco.com

- **Overview**
- **Link-State Routing Protocols**
- **Defining an OSPF Area**
- **Defining OSPF Adjacencies**
- **OSPF Calculation**
- **Summary**
- **Quiz**

Link-State Routing Protocols

This topic defines and describes link-state routing protocols, including OSPF and Intermediate System-to-Intermediate System Protocol (IS-IS).



The need to overcome limitations of distance vector routing protocols led to the development of link-state routing protocols. Link-state routing protocols have the following characteristics:

- Respond quickly to network changes
- Send triggered updates when a network change occurs
- Send periodic updates, known as link-state refresh, at long intervals, such as every 30 minutes

Link-state routing protocols generate routing updates only when a change occurs in the network topology. When a link changes state, the device that detected the change creates a link-state advertisement (LSA) concerning that link. The LSA propagates to all neighboring devices using a special multicast address. Each routing device takes a copy of the LSA, updates its link-state database, and forwards the LSA to all neighboring devices. This flooding of the LSA ensures that all routing devices update their databases before updating routing tables to reflect the new topology.

The link-state database is used in calculating the best paths through the network. Link-state routers find the best paths to a destination by applying Dijkstra's algorithm, also known as SPF, 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.

Link-State Routing Protocols

Cisco.com

- **Link-state routers recognize more information about the network than their distance vector counterparts.**
- **Consequently link-state routers tend to make more accurate decisions.**
- **Link-state routers keep track of the following:**
 - Their neighbors
 - All routers within the same area
 - Best paths toward a destination

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-8

OSPF and IS-IS are classified as link-state routing protocols because of the manner in which they distribute routing information and calculate routes.

Link-state routing protocols collect routing information from all other routers in the network or from within a defined area of the network. Once link-state routing protocols have collected this information from all routers, each router independently calculates its best paths to all destinations in the network using Dijkstra's algorithm. Incorrect information from any particular router is less likely to cause confusion, because each router maintains its own view of the network.

Link-State Data Structures

Cisco.com

- **Neighbor table:**
 - Also known as the adjacency database
(list of recognized neighbors)
- **Topology table:**
 - Typically referred to as LSDB
(routers and links in the area or network)
 - All routers within an area have an identical LSDB
- **Routing table:**
 - Commonly named a forwarding database
(list of best paths to destinations)

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 4-6

For consistent routing decisions to be taken by all the routers in the network, each router must keep a record of the following information:

- **Its immediate neighbor routers:** If the router loses contact with a neighboring router, within a few seconds, it will invalidate all paths through that router and recalculate its paths through the network. Adjacency information about neighbors is stored in the neighbor table, also known as an adjacency database, in OSPF.
- **All the other routers in the network, or in its area of the network, and their attached networks:** The router recognizes other routers and networks through LSAs, which are flooded through the network. LSAs are stored in a topology table, also called a link-state database (LSDB).
- **The best paths to each destination:** Each router independently calculates best paths to each destination in the network using Dijkstra's algorithm. The best paths are then offered to the routing table or forwarding database. Packets arriving at the router are forwarded based on the information held in the routing table.

The memory resources needed to maintain these tables is one drawback to link-state protocols. However, because the topology table is identical for all OSPF routers in an area and contains full information about all the routers and links in an area, each router is able to independently select a loop-free and efficient pathway, based on cost, to reach every network in the area. This benefit overcomes the “routing by rumors” limitations of distance vector routing.

Example

With distance vector routing protocols, the routers rely on routing decisions from the neighbors. Routers do not have a full picture of the network topology.

With link-state routing protocols, each router has a full picture of the network topology, and each router can independently make a decision based on an accurate picture of the network topology.

Defining an OSPF Area

This topic describes the two-layer hierarchy structure of OSPF.

Link-State Data Structure: Network Hierarchy

Cisco.com

Link-state routing requires a hierarchical network structure that is enforced by OSPF.

This two-level hierarchy consists of the following:

- **Transit area (backbone or area 0)**
- **Regular areas (nonbackbone areas)**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

In small networks, the web of router links is not complex, and paths to individual destinations are easily deduced. However, in large networks, the resulting web is highly complex, and the number of potential paths to each destination is large. Therefore, the Dijkstra calculations comparing all these possible routes can be very complex and can take significant time.

Link-state routing protocols usually reduce the size of the Dijkstra calculations by partitioning the network into areas. The number of routers in an area and the number of LSAs that flood only within the area are small, which means that the link-state or topology database for an area is small. Consequently, the Dijkstra calculation is easier and takes less time. Link-state routing protocols use a two-layer area hierarchy as follows:

- **Transit area:** An OSPF area whose primary function is the fast and efficient movement of IP packets. Transit areas interconnect with other OSPF area types. Generally, end users are not found within a transit area. OSPF area 0, also known as the backbone area, is by definition a transit area.
- **Regular area:** An OSPF area whose primary function is to connect users and resources. Regular areas are usually set up along functional or geographical groupings. By default, a regular area does not allow traffic from another area to use its links to reach other areas. All traffic from other areas must cross a transit area such as area 0. An area that does not allow traffic to pass through it is known as a regular area, or nonbackbone area, and can have a number of subtypes, including stub area, totally stubby area, and not-so-stubby area (NSSA).

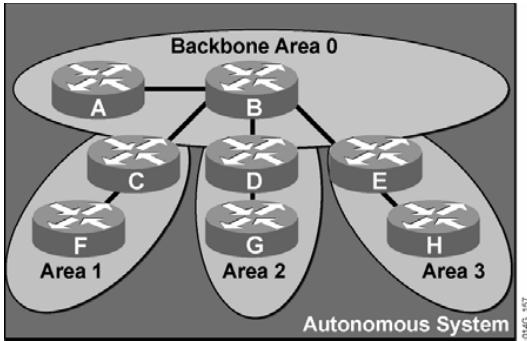
OSPF forces a rigid two-layer area hierarchy. The underlying physical connectivity of the network must map to the two-layer area structure, with all nonbackbone areas attaching directly to area 0.

OSPF Areas

Cisco.com

OSPF area characteristics:

- Minimizes routing table entries
- Localizes impact of a topology change within an area
- Detailed LSA flooding stops at the area boundary
- Requires a hierarchical network design



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-8

In link-state routing protocols, all routers must keep a copy of the LSDB; the more OSPF routers, the larger the LSDB. It can be advantageous to have all information in all routers, but this approach does not scale to large network sizes. The area concept is a compromise. Routers inside an area maintain detailed information about the links and only general or summary information about routers and links in other areas.

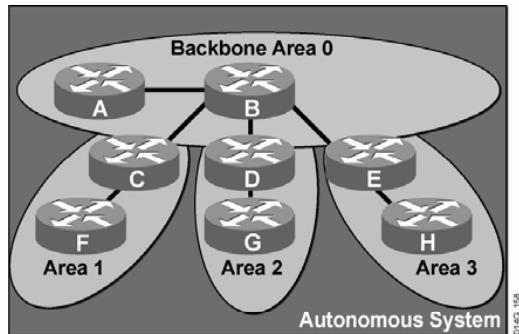
When a router or link fails, that information is flooded along adjacencies only to the routers in the local area. Routers outside the area do not receive this information. By maintaining a hierarchical structure and limiting the number of routers in an area, an OSPF autonomous system can scale to very large sizes.

OSPF areas require a hierarchical structure, meaning that all areas must connect directly to area 0. In the figure, notice that links between area 1 routers and area 2 or 3 routers are not allowed. All interarea traffic must pass through the backbone area, area 0. The optimal number of routers per area varies based on factors such as network stability, but it is recommended that there be no more than 50 to 100 routers per area.

Area Terminology

Cisco.com

- Routers A and B are backbone routers.
- Backbone routers make up area 0.
- Routers C, D, and E are known as Area Border Routers (ABRs).
- ABRs attach all other areas to area 0.



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

Routers that make up area 0 are known as backbone routers. Hierarchical networking defines area 0 as the core. All other areas connect directly to backbone area 0.

An area border router (ABR) connects area 0 to the nonbackbone areas. An OSPF ABR plays a very important role in network design. An ABR has the following characteristics:

- Separates LSA flooding zones
- Becomes the primary point for area address summarization
- Functions regularly as the source for default routes
- Maintains the LSDB for each area with which it is involved

The ideal design is to have each ABR connected to two areas only, the backbone and another area, with three areas being the upper limit.

Defining OSPF Adjacencies

Before sending updates, neighboring routers must form a logical adjacency. This topic introduces the concept of an OSPF adjacency.

LS Data Structures: Adjacency Database

Cisco.com

- **Routers discover neighbors by exchanging hello packets.**
- **Routers declare neighbors to be up after checking certain parameters or options in the hello packet.**
- **Point-to-point WAN links:**
 - Both neighbors become fully adjacent.
- **LAN links:**
 - Neighbors form an adjacency with the DR and BDR.
 - Maintain two-way state with the other routers (DROTHERs).
- **Routing updates and topology information are passed only between adjacent routers.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-10

A router running a link-state routing protocol must first establish neighbor adjacencies with its neighboring routers. A router achieves this neighbor adjacency by exchanging hello packets with the neighboring routers. In general, routers establish adjacencies as follows:

1. The router sends and receives hello packets to and from its neighboring routers. The format of the destination address is typically multicast.
2. The routers exchange hello packets subject to protocol-specific parameters, such as checking whether the neighbor is in the same autonomous system and area. Routers declare the neighbor up when the exchange is complete.
3. After two routers establish neighbor adjacency using the hello packets, they synchronize their LSDBs by exchanging LSAs and confirming the receipt of LSAs from the adjacent router. The two neighboring routers now recognize that they have synchronized their LSDBs with each other. For OSPF, the routers are now in full adjacency state with each other.
4. If necessary, the routers forward any new LSAs to other neighboring routers, ensuring complete synchronization of link-state information inside the area.

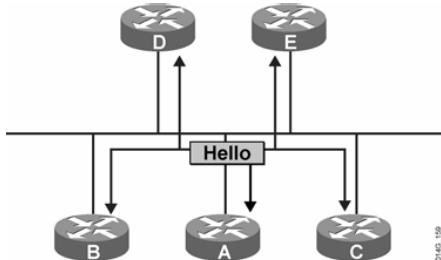
The two OSPF routers on a point-to-point serial link, usually encapsulated in High-Level Data Link Control (HDLC) or PPP, form a full adjacency with each other.

LAN links elect one router as the designated router (DR) and another as the backup designated router (BDR). All other routers on the LAN form full adjacencies with these two routers and pass LSAs only to them. The DR forwards the updates from one neighbor on the LAN to all

other neighbors on that LAN. One of the main functions of a DR is that all of the routers on the same LAN have an identical database, and the DR passes its database to any new routers that come up. It is inefficient to have all the routers on that LAN pass the same information to the new router, so one router represents the other routers to a new router on the LAN or to other routers in the area. The routers also maintain a partial-neighbor relationship, a two-way adjacency state, with the other routers on the LAN that are not the DR or BDR (DROTHERs).

OSPF Adjacencies

Cisco.com



Routers build logical adjacencies between each other using the Hello Protocol. Once an adjacency is formed:

- LSDB packets are exchanged to synchronize each other's LSDBs.
- LSAs are flooded reliably throughout the area or network using these adjacencies.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-11

The exchange of link-state information occurs through LSAs, which are also known as link-state protocol data units (PDUs). LSAs report the state of routers and the links between routers, hence the term *link state*. Link-state information must be synchronized between routers, which means the following:

- LSAs are reliable; there is a method for acknowledging the delivery of LSAs.
- LSAs are flooded throughout the area or throughout the domain if there is no area structure.
- LSAs have a sequence number and a set lifetime so that each router recognizes that it has the most up-to-date version of the LSA.
- LSAs are periodically refreshed to confirm topology information before it ages out of the link-state database.

Only by reliably flooding link-state information can every router in the area or domain ensure that it has the latest, most accurate view of the network. Only by having the latest and most accurate view of the network can the router make reliable routing decisions that are consistent with the decisions of other routers in the network.

OSPF Calculation

This topic describes the SPF calculation used by OSPF to find the best path to each destination network. The best paths are then populated in the routing table.

OSPF Calculation

Cisco.com

Routers find the best paths to destinations by applying Dijkstra's SPF algorithm to the link-state database as follows:

- **Every router in an area has the identical link-state database.**
- **Each router in the area places itself into the root of the tree that is built.**
- **The best path is calculated with respect to the lowest total cost of links to a specific destination.**
- **Best routes are put into the forwarding database.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

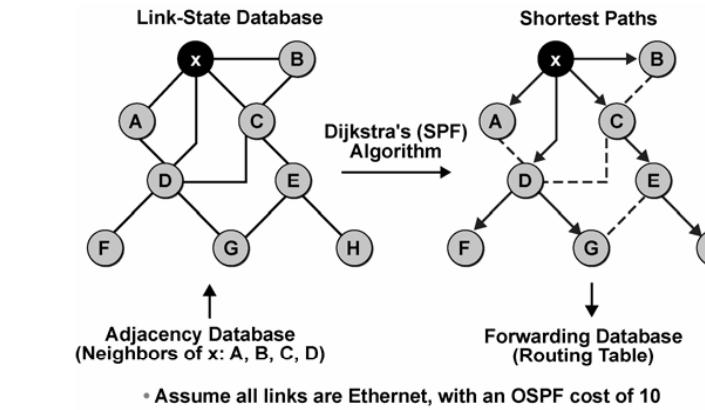
Edsger Dijkstra designed a mathematical algorithm for calculating the best paths through complex networks. Link-state routing protocols use Dijkstra's algorithm to calculate the best paths through a network.

By assigning a cost to each link in the network and by placing the specific node at the root of a tree and summing the costs toward each given destination, the branches of the tree can be calculated.

For OSPF, the default behavior is that the interface cost is calculated based on its configured bandwidth. An OSPF cost can also be manually defined for each interface, which will override the default cost value calculated based on the configured bandwidth.

SPF Calculation

Cisco.com

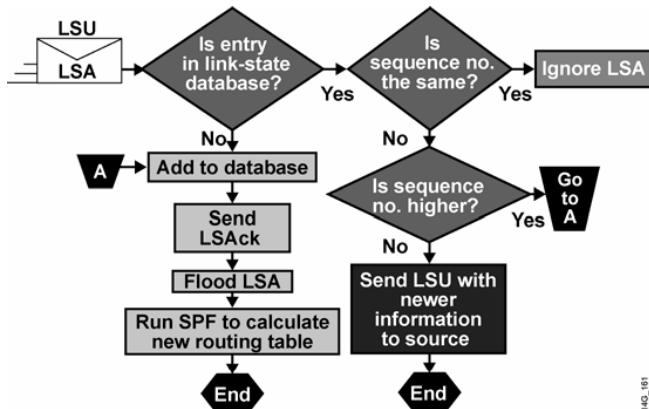


The figure illustrates an example of a Dijkstra calculation. The Dijkstra calculation occurs as follows:

- Router H advertises its presence to router E; router E then passes on the advertisements of H and its own advertisements to its neighbors (C and G); router G passes these and its own advertisements on to D; and so on.
- These LSAs follow the split horizon rule, which dictates that a router should never advertise an LSA to the router from which it came. In the example, router E does not advertise the LSAs of router H back to H.
- Router x has four neighboring routers: A, B, C, and D. From these routers, it receives the LSAs for all other routers in the network. From these LSAs, it can also deduce the links between all routers and draw the web of routers depicted in the figure.
- Each Ethernet link in the figure is assigned an OSPF cost of 10. By summing the costs to each destination, the router can deduce the best path to each destination.
- The right side of the figure shows the resulting best paths (the SPF tree). From these best paths, routes to destination networks attached to each router are offered to the routing table; for each route, the next-hop address is the appropriate neighboring router (A, B, C, or D).

LS Data Structures: LSA Operation

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-17

DHQ_161

Each LSA entry has its own aging timer, which the link-state age field carries. The default timer value for OSPF is 30 minutes (expressed in seconds in the link-state age field).

After an LSA entry ages, the router that originated the entry sends a link-state update (LSU) about the network to verify that the link is still active. The LSU can contain one or more LSAs.

The LSA validation method saves on bandwidth compared to distance vector routers, which send their entire routing table at short periodic intervals.

When each router receives the LSU, it does the following:

- If the entry does not already exist, the router adds the entry to its link-state database, sends a link-state acknowledgment (LSAck) back, floods the information to other routers, runs SPF, and updates its routing table.
- If the entry already exists and the received LSU has the same information, the router ignores the LSA entry.
- If the entry already exists but the LSU includes newer information, the router adds the entry to its link-state database, sends an LSACK back, floods the information to other routers, runs SPF, and updates its routing table.
- If the entry already exists but the LSU includes older information, it sends an LSU to the sender with its newer information.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **OSPF is a link-state routing protocol that builds three tables: neighbor table, link-state topology database, and routing table or forwarding database.**
- **A two-tier hierarchical network structure is used by OSPF in which the network is divided into areas. This area structure is used to separate the LSDB into more manageable sizes.**
- **Adjacencies are built by OSPF routers using the Hello Protocol. Over these logical adjacencies, LSUs are sent to exchange database information between adjacent OSPF routers.**
- **Dijkstra's SPF algorithm is used to calculate best paths for all destinations. SPF is run against the LSDB, and the outcome is a table of best paths known as the routing table.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-18

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 table is NOT maintained by a link-state routing protocol?

- A) routing
- B) topology
- C) update
- D) neighbor

Q2) The memory needed to maintain tables is one disadvantage of link-state protocols.

- A) true
- B) false

Q3) Match each table to its function.

- A) routing
- B) topology
- C) neighbor

- _____ 1. stores LSAs
- _____ 2. stores adjacencies
- _____ 3. stores best paths

Q4) Which term refers to the router that connects area 0 to a nonbackbone area?

- A) area boundary router
- B) area border router
- C) autonomous system boundary router
- D) backbone router

Q5) What is the recommended guideline for the number of routers per OSPF area?

- A) 50 to 100
- B) 10 to 20
- C) 200 to 400
- D) 500 to 1000

- Q6) Which OSPF packet helps form the neighbor adjacency?
- A) exchange packet
 - B) hello packet
 - C) neighbor discovery packet
 - D) adjacency packet
- Q7) Which criterion does SPF use to determine the best path?
- A) lowest delay
 - B) highest bandwidth
 - C) lowest total cost of the route
 - D) total bandwidth of the route
- Q8) Which table is populated as a result of the SPF calculations?
- A) topology
 - B) routing
 - C) adjacency
 - D) neighbor

Quiz Answer Key

- Q1) C
Relates to: Link-State Routing Protocols
- Q2) A
Relates to: Link-State Routing Protocols
- Q3) 1-B, 2-C, 3-A
Relates to: Link-State Routing Protocols
- Q4) B
Relates to: Defining an OSPF Area
- Q5) A
Relates to: Defining an OSPF Area
- Q6) B
Relates to: Defining OSPF Adjacencies
- Q7) C
Relates to: OSPF Calculation
- Q8) B
Relates to: OSPF Calculation

OSPF Packet Types

Overview

The OSPF protocol has five packet types: hello, database description (DBD), link-state request (LSR), link-state update (LSU), and link-state acknowledgment (LSAck). This module defines each packet and explains where and how these packets interact to build OSPF neighbor adjacencies and maintain the OSPF topology database.

Relevance

The five OSPF packet types enable all OSPF information flow between routers. Without having packet formats defined, routers cannot properly exchange and interpret the information.

Objectives

Upon completing this lesson, you will be able to:

- List the types of OSPF packets
- Explain how neighbor adjacencies are established in OSPF
- Identify the exchange process and the neighbor adjacency states of OSPF
- Define OSPF LSU sequence numbers
- Use the **debug ip ospf packet** command

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Knowledge of IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

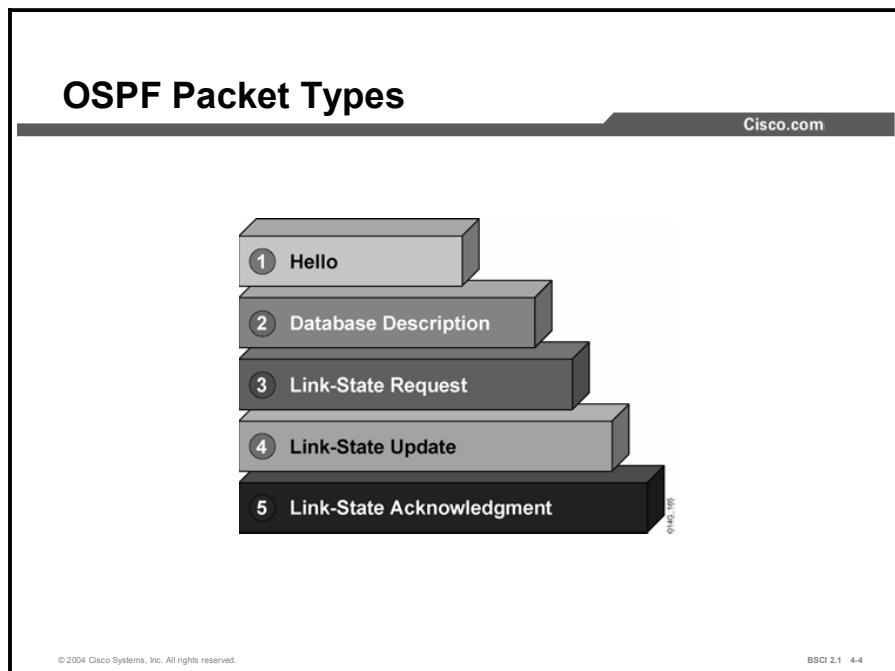
Outline

Cisco.com

- **Overview**
- **Types of OSPF Packets**
- **OSPF Neighbor Adjacency Establishment**
- **Exchange Process and OSPF Neighbor Adjacency States**
- **OSPF Link-State Sequence Numbers**
- **The debug ip ospf packet command**
- **Summary**
- **Quiz**

Types of OSPF Packets

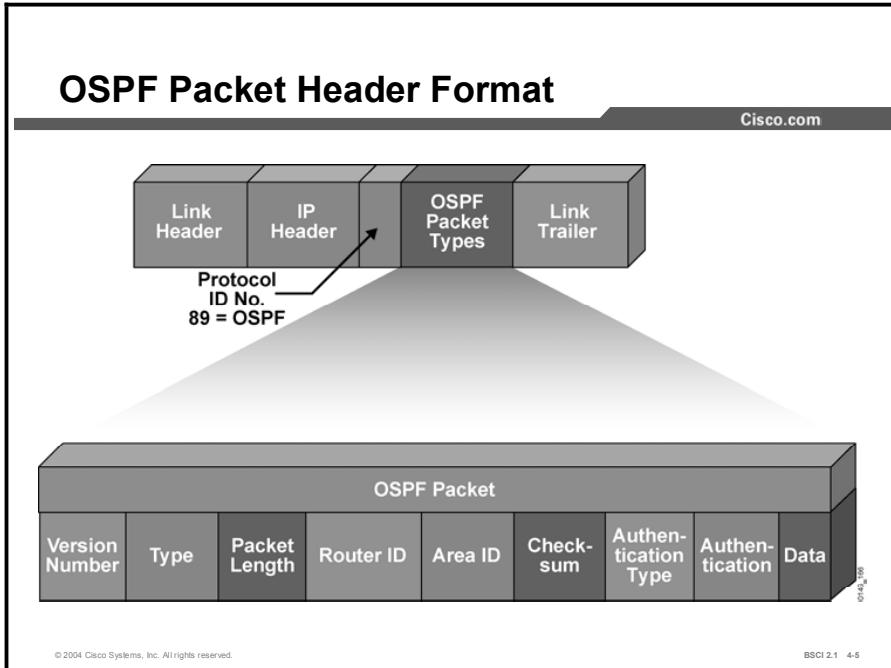
This topic gives a general description of each of the five OSPF packet types.



All five packet types are used in the normal operation of OSPF. The table contains descriptions of each type.

OSPF Packets

Type	Packet Name	Description
1	Hello	Builds adjacencies between neighbors
2	DBD	Checks for database synchronization between routers
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types



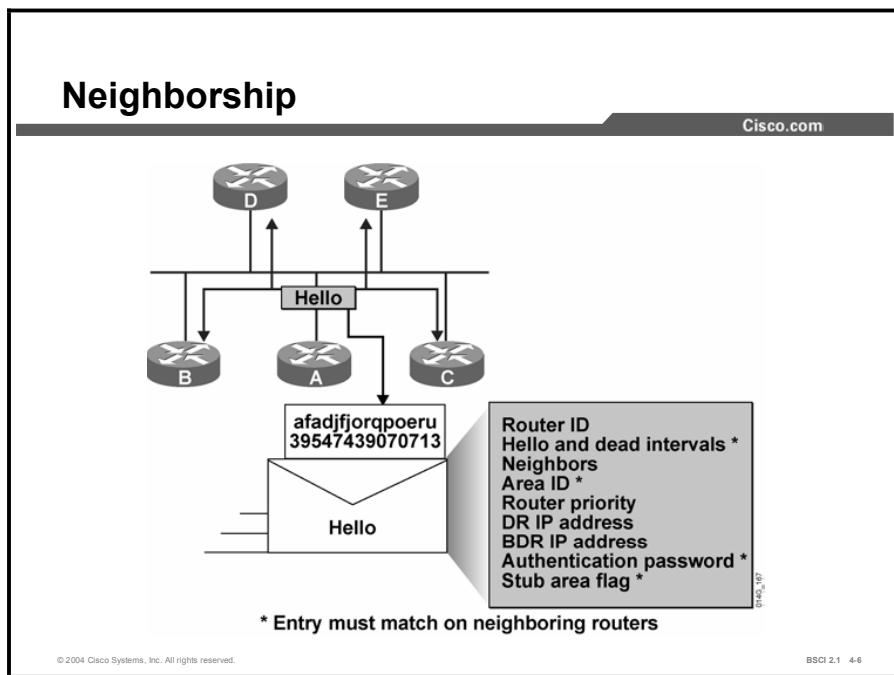
All five OSPF packets are encapsulated directly into an IP payload. The OSPF packet does not use TCP or User Datagram Protocol (UDP). OSPF requires a reliable packet transport scheme and because TCP is not used, it has defined its own acknowledgment routine using an acknowledgment packet (OSPF packet type 5).

In the IP header, a protocol identifier of 89 defines all OSPF packets. Each of the OSPF packets begins with the same header format. This header has the following fields:

- **Version number:** For OSPF version 2
- **Packet type:** Differentiates the five OSPF packet types
- **Packet length:** Length of OSPF packet in bytes
- **Router ID:** Defines which router is the source of the packet
- **Area ID:** Defines the area where the packet originated
- **Checksum:** Used for packet-header error-detection to ensure that the OSPF packet was not corrupted during transmission
- **Authentication type:** An option in OSPF that describes either clear-text passwords or encrypted Message Digest 5 (MD5) formats for router authentication
- **Data (for hello packet):** Contains a list of known neighbors
- **Data (for DBD packet):** Contains a summary of the link-state database (LSDB), which includes all known router IDs and their last sequence number, among a number of other fields
- **Data (for LSR packet):** Contains the type of LSU needed and the router ID of the needed LSU
- **Data (for LSU packet):** Contains the full link-state advertisement (LSA) entry. Multiple LSA entries can fit in one OSPF update packet
- **Data (for LSAck packet):** Is empty

OSPF Neighbor Adjacency Establishment

The Hello protocol builds the neighbor list in a router. Once this process is accomplished, the Hello protocol then forms a logical adjacency between some of the routers depending on link type. This topic describes the Hello protocol, types of links, and how an adjacency is formed.



Neighbor OSPF routers must recognize each other on the network before they can share information because OSPF routing depends on the status of the link between two routers. This process is done using the Hello protocol. The Hello protocol establishes and maintains neighbor relationships by ensuring bidirectional (two-way) communication between neighbors. Bidirectional communication occurs when a router recognizes itself listed in the hello packet received from a neighbor.

Each interface participating in OSPF uses IP multicast address 224.0.0.5 to send hello packets periodically. A hello packet contains the following information:

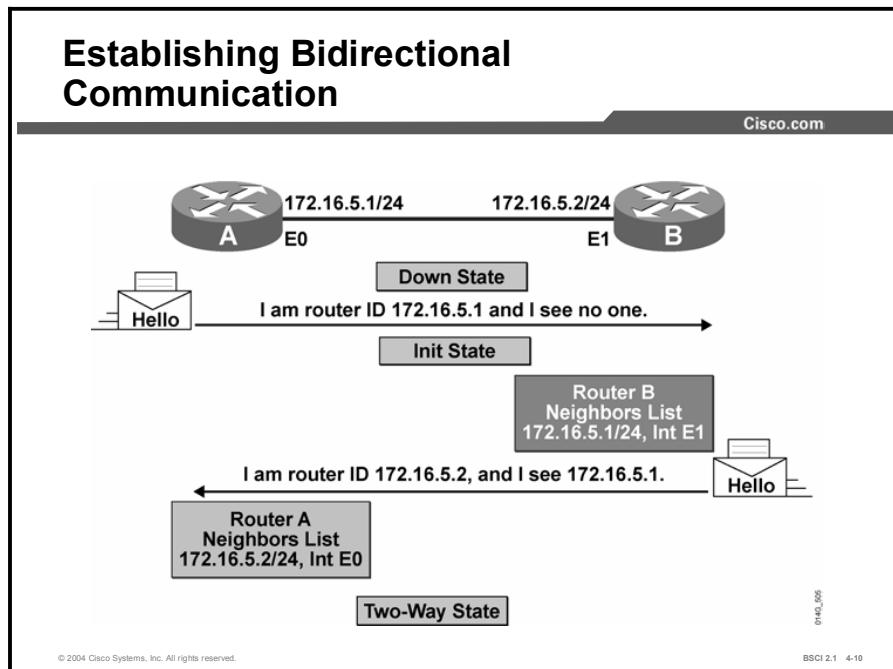
- **Router ID:** A 32-bit number that uniquely identifies the router. The highest IP address on an active interface is chosen by default unless a loopback interface or the router ID is configured; for example, IP address 172.16.12.1 would be chosen over 172.16.1.1. This identification is important in establishing neighbor relationships and coordinating LSU exchanges. Also, the router ID breaks ties during the DR and BDR selection processes if the OSPF priority values are equal.
- **Hello and dead intervals:** The hello interval specifies the frequency in seconds that a router sends hello packets (10 seconds is the default on multiaccess networks). The dead interval is the time in seconds that a router waits to hear from a neighbor before declaring the neighboring router out of service (four times the hello interval by default). These timers must be the same on neighboring routers.
- **Neighbors:** The neighbors field lists the adjacent routers with established bidirectional communication. This bidirectional communication is indicated when the router recognizes itself listed in the neighbors field of the hello packet from the neighbor.

- **Area ID:** To communicate, two routers must share a common segment, and their interfaces must belong to the same OSPF area on that segment (they must also share the same subnet and mask). These routers will all have the same link-state information.
- **Router priority:** An 8-bit number that indicates the priority of a router. Priority is used when selecting a DR and BDR.
- **DR and BDR IP addresses:** If they are known, this field gives the IP addresses of the DR and BDR for the specific network.
- **Authentication password:** If router authentication is enabled, two routers must exchange the same password. Authentication is not required, but if it is enabled, all peer routers must have the same password.
- **Stub area flag:** A stub area is a special area. Two routers must agree on the stub area flag in the hello packets. Designating a stub area is a technique that reduces routing updates by replacing them with a default route.

Note After a DR and BDR are selected, any router added to the network will establish adjacencies with the DR and BDR only.

Exchange Process and OSPF Neighbor Adjacency States

Once a bidirectional adjacency is formed, OSPF must exchange and synchronize the LSDBs between routers. This topic defines the process of exchanging and synchronizing the LSDBs between routers.



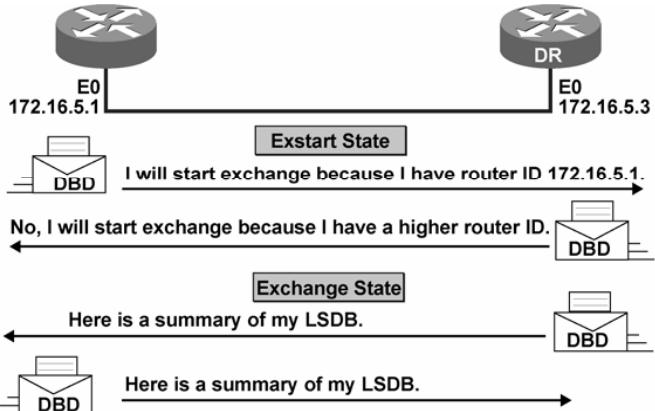
When routers running OSPF initialize, an exchange process using the Hello protocol is the first procedure. The exchange process that happens when routers are coming up on the network is as follows:

- Step 1** Router A is enabled on the LAN and is in a down state because it has not exchanged information with any other router. It begins by sending a hello packet through each of its interfaces participating in OSPF, even though it does not know the identity of the DR or of any other routers. The hello packet is sent out using the multicast address 224.0.0.5.
- Step 2** All directly connected routers running OSPF receive the hello packet from router A and add router A to their list of neighbors. This state is the initial state (init).
- Step 3** All routers that received the hello packet send a unicast reply hello packet to router A with their corresponding information. The neighbor field in the hello packet includes all other neighboring routers, including router A.
- Step 4** When router A receives these hello packets, it adds all the routers that had its router ID in their hello packets to its own neighbor relationship database. This state is referred to as the two-way state. At this point, all routers that have each other in their lists of neighbors have established bidirectional communication.

- Step 5** If the link type is a broadcast network, generally a LAN link like Ethernet, then you must first select a DR and BDR. The DR forms the bidirectional adjacencies between all other routers on the LAN link. This process must occur before the routers can begin exchanging link-state information.
- Step 6** Periodically (every 10 seconds by default on broadcast networks) the routers within a network exchange hello packets to ensure that communication is still working. The hello updates include the DR, BDR, and the list of routers whose hello packets have been received by the router. Remember that “received” means that the receiving router recognizes its name as one of the entries in the received hello packet.

Discovering the Network Routes

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

When routers running OSPF initialize, an exchange process using the Hello protocol is the first step. After the DR and BDR have been selected, the routers are considered to be in the exstart state and they are ready to discover the link-state information about the internetwork and create their LSDBs. The process used to discover the network routes is the exchange protocol, and it gets the routers to a full state of communication. The first step in this process is for the DR and BDR to establish adjacencies with each of the other routers. Once adjacent routers are in a full state, they do not repeat the exchange protocol unless the full state changes.

The exchange protocol operates as follows:

- Step 1** In the exstart state, the DR and BDR establish adjacencies with each router in the network. During this process, a master-slave relationship is created between each router and its adjacent DR and BDR. The router with the higher router ID acts as the master during the exchange process.

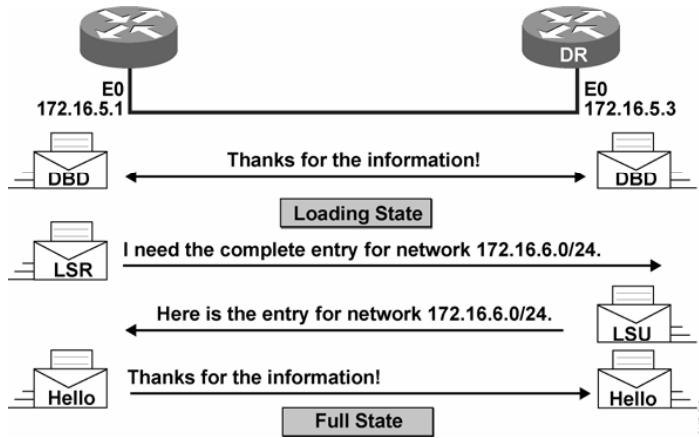
Note	Note that only the DR exchanges and synchronizes link-state information with the routers to which it has established adjacencies. Having the DR represent the network in this capacity reduces the amount of routing update traffic.
-------------	--

- Step 2** The master and slave routers exchange one or more DBD packets. The routers are in the exchange state.

A DBD includes information about the LSA entry header that appears in the LSDB of the router. The entries can be about a link or about a network. Each LSA entry header includes information about the link-state type, the address of the advertising router, the cost of the link, and the sequence number. The router uses the sequence number to determine the “newness” of the received link-state information.

Adding the Link-State Entries

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-15

Step 3 When routers running OSPF initialize, an exchange process uses the Hello protocol.. When the router receives the DBD, it performs the following actions:

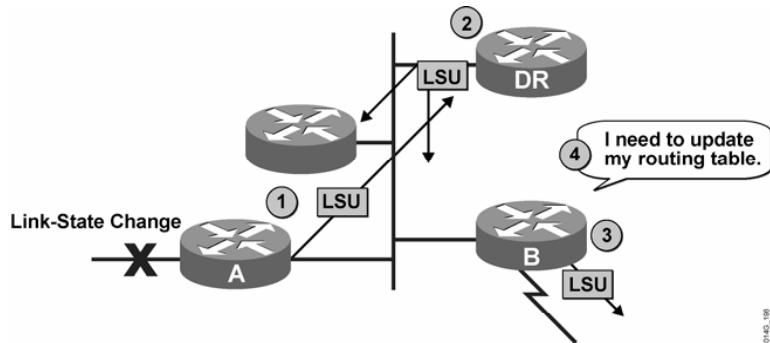
1. It acknowledges the receipt of the DBD using the LSAck packet.
2. It compares the information it received with the information it has. If the DBD has a more up-to-date link-state entry, then the router sends an LSR to the other router. The process of sending LSRs is called the loading state.
3. The other router responds with the complete information about the requested entry in an LSU packet. Again, when the router receives an LSU, it sends an LSAck.

Step 4 The router adds the new link-state entries to its LSDB.

Once all LSRs have been satisfied for a given router, the adjacent routers are considered synchronized and in a full state. The routers must be in a full state before they can route traffic. At this point, all the routers in the area should have identical LSDBs.

Maintaining Routing Information

Cisco.com



- Router A notifies all OSPF DRs on 224.0.0.6.
- DR notifies others on 224.0.0.5.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 4-19

In a link-state routing environment, it is very important for the LSDBs (topology tables) of all routers to stay synchronized. When there is a change in a link state, the routers use a flooding process to notify the other routers in the network of the change. LSUs provide the mechanism for flooding LSAs.

Note Although it is not shown in this figure, all LSUs are acknowledged.

In general, the following are the flooding process steps in a multiaccess network:

- Step 1** A router notices a change in a link state and multicasts an LSU packet that includes the updated LSA entry to 224.0.0.6, to all OSPF DRs and BDRs. An LSU packet may contain several distinct LSAs.
- Step 2** The DR acknowledges the receipt of the change and floods the LSU to others on the network using the OSPF multicast address 224.0.0.5. After receiving the LSU, each router responds to the DR with an LSAck. To make the flooding procedure reliable, each LSA must be acknowledged separately.
- Step 3** If a router is connected to another network, it floods the LSU to other networks by forwarding the LSU to the DR of the multiaccess network or to the adjacent router if it is in a point-to-point network. The DR, in turn, multicasts the LSU to the other routers in the network.
- Step 4** The router updates its LSDB using the LSU that includes the changed LSA. It then recomputes the SPF algorithm against the updated database after a short delay (the SPF delay) and updates the routing table as necessary.

OSPF simplifies the synchronization issue by requiring only adjacent routers to remain synchronized.

Summaries of individual link-state entries, not the complete link-state entries, are sent every 30 minutes to ensure LSDB synchronization. Each link-state entry has a timer to determine when the LSA refresh update must be sent.

Each link-state entry also has a maximum age of 60 minutes. If a link-state entry has not been refreshed within 60 minutes, it is removed from the LSDB.

Note In a Cisco router, if a route already exists, the routing table is used at the same time the SPF algorithm is calculating. However, if the SPF is calculating a new route, the use of the new route occurs after the SPF calculation is complete.

OSPF Link-State Sequence Numbers

A combination of the maximum age (maxage) and refresh timers and link-state sequence numbers helps OSPF maintain a database of only the most recent link-state records. This topic describes the process of maintaining a database of only the most recent link-state records.

LSA Sequence Numbering

Cisco.com

- **Each LSA record in the LSDB maintains a sequence number.**
- **The sequence numbering scheme is a 4-byte number that begins with 0x80000001 and ends with 0x7fffffff.**
- **OSPF floods each LSA record every 30 minutes to maintain proper database synchronization. Each time the LSA is flooded, the sequence number is incremented by one.**
- **Ultimately, an LSA sequence number will wrap around to 0x80000001. When this occurs, the existing LSA is prematurely aged to maxage (one hour) and flushed.**
- **When a router encounters two instances of an LSA, it must determine which is more recent. The LSA having the newer (higher) LS sequence number is more recent.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-20

The sequence number field in a link-state record is 32 bits in length. Beginning with the left-most bit set, the first legal sequence number is 0x80000001. It is used to detect old or redundant LSA records. The larger the number, the more recent the LSA.

To ensure an accurate database, OSPF floods (refreshes) each LSA record every 30 minutes. Each time a record is flooded, the sequence number is incremented by one. An LSA record will reset its maximum age when it receives a new LSA update. An LSA will never remain longer in the database than the maximum age of one hour without a refresh.

It is possible for an LSA to remain in the database for long periods of time, being refreshed every 30 minutes. At some point the sequence number will need to wrap back to the starting sequence number.

When this process occurs, the existing LSA will be prematurely aged out (the maxage timer immediately set to one hour) and flushed. The LSA will then begin its sequencing at 0x80000001 again.

LSA Sequence Numbers and Maximum Age

Cisco.com

```
RTC# show ip ospf database
OSPF Router with ID (203.250.15.67) (Process ID 10)
  Router Link States (Area 1)
Link ID      ADV Router      Age    Seq#      Checksum  Link count
203.250.15.67  203.250.15.67  48  0x80000008  0xB112      2
203.250.16.130  203.250.16.130  212  0x80000006  0x3F44      2
```

- Every OSPF router announces a router LSA for those interfaces that it owns in that area.
- Link ID is the ID of the router that created the router LSA.
- The advertising router (shown as “ADV Router” in the output) is the router ID of the OSPF router that announced the router LSA. Generally, the link ID and advertising router for a router LSA are the same.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-21

The output of the **show ip ospf database** command shown in the figure is an example of how the link-state age and link-state sequence numbers are kept in the database. The first router LSA entry in the OSPF database suggests that the router LSA with link ID 203.250.15.67 has been updated eight times (because the sequence number is 0x80000008) and that the last update occurred 48 seconds ago.

The debug ip ospf packet Command

This topic describes the use of the **debug** tool to decode and better understand OSPF handshakes and packet formats.

debug ip ospf packet

Cisco.com

Debug of a single packet

```
Router# debug ip ospf packet
OSPF: rcv. v:2 t:1 1:48 rid:200.0.0.117
      aid:0.0.0.0 chk:6AB2 aut:0 auk:
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-22

The **debug ip ospf packet** command is used in troubleshooting and to verify that OSPF packets are flowing properly between two routers.

The output of this **debug** command is shown in the figure. Notice that the fields in the OSPF header are not described in any detail. The table lists each field of an OSPF packet header.

OSPF Packet Header Fields

Field	Description
v:	Provides the version of OSPF
t:	Specifies the OSPF packet type: 1: hello 2: DBD 3: LSR 4: LSU 5: LSAck
l:	Specifies the OSPF packet length in bytes
rid:	Provides the OSPF router ID
aid:	Shows the OSPF area ID
chk:	Displays the OSPF checksum
aut:	Provides the OSPF authentication type: 0: No authentication 1: Simple password 2: MD5
auk:	Specifies the OSPF authentication key
keyid:	Displays the MD5 key ID
seq:	Provides the sequence number

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- There are five OSPF packet types: hello, DBD, LSU, LSR, and LSAck.
- The Hello protocol forms logical neighbor and adjacency relationships. A designated router may be required to coordinate adjacency formations.
- The exchange protocol passes through several states, init, two-way, exstart, and exchange, before finally reaching the goal of full state. Full state means that databases are synchronized with adjacent routers.
- Link-state records are advertised on change but are also sent every 30 minutes to ensure database integrity. The maximum time an LSR will stay in the database, without an update, is one hour. The LSR increments its sequence number every time it is advertised.

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 IP protocol number for OSPF packets?

- A) 89
- B) 86
- C) 20
- D) 76

Q2) Which packet is NOT an OSPF packet type?

- A) LSU
- B) LSR
- C) DBD
- D) LSAck
- E) hello
- F) query

Q3) Which multicast address does the Hello protocol use?

- A) 224.0.0.5
- B) 224.0.0.6
- C) 224.0.0.7
- D) 224.0.0.8

Q4) The Hello protocol sends periodic updates to ensure that a neighbor relationship is maintained between adjacent routers.

- A) true
- B) false

Q5) Place the exchange protocol states in the correct order.

- A) _____ two-way
- B) _____ loading
- C) _____ down
- D) _____ full
- E) _____ exchange
- F) _____ init
- G) _____ exstart

Q6) DBD packets are involved during which two states? (Choose two.)

- A) exstart
- B) loading
- C) exchange
- D) two-way

Q7) At which interval does OSPF refresh LSAs?

- A) 10 seconds
- B) 30 seconds
- C) 30 minutes
- D) 1 hour

Q8) Which field is NOT a field within an OSPF packet header?

- A) packet length
- B) router ID
- C) authentication type
- D) maxage time

Quiz Answer Key

Q1) A

Relates to: Types of OSPF Packets

Q2) F

Relates to: Types of OSPF Packets

Q3) A

Relates to: OSPF Neighbor Adjacency Establishment

Q4) A

Relates to: OSPF Neighbor Adjacency Establishment

Q5) A-3, B-6, C-1, D-7, E-5, F-2, G-4

Relates to: Exchange Process and OSPF Neighbor Adjacency States

Q6) A, C

Relates to: Exchange Process and OSPF Neighbor Adjacency States

Q7) C

Relates to: OSPF Link-State Sequence Numbers

Q8) D

Relates to: The debug ip ospf packet Command

Configuring Basic OSPF

Overview

This lesson discusses the primary configuration commands for a single-area OSPF design and how to configure the **router ospf** and **network** commands. The **network** command for OSPF requires a special inverse mask technique that is defined in this lesson.

Relevance

Many OSPF networks require only a single area. This lesson discusses the key commands for a single-area OSPF network. Basic OSPF configuration is considered to be beginner-level configuration knowledge.

Objectives

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

- Configure and verify a basic single-area OSPF design
- Use OSPF configuration commands to properly enable the OSPF routing process

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Understanding of IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Configuring Basic Single-Area OSPF**
- **Manipulating the OSPF Router ID**
- **Summary**
- **Quiz**

Configuring Basic Single-Area OSPF

This topic describes the two-step process to configure basic OSPF.

Configuring Basic OSPF: Single Area

Cisco.com

```
Router(config)#  
router ospf process-id
```

- Turns on one or more OSPF routing processes in the Cisco IOS software.

```
Router(config-router)#  
network address inverse-mask area [area-id]
```

- Router OSPF subordinate command that defines the interfaces (by network number) that OSPF will run on. Each network number must be defined to a specific area.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-4

To configure the OSPF process, complete the following steps:

Step 1 Enable the OSPF process on the router using the **router ospf** command as follows:

```
router(config)# router ospf process-id
```

The table describes the process-id parameter of this command.

router ospf Parameter

Parameter	Description
<i>process-id</i>	An internally used number to identify the OSPF routing process. The process ID does not need to match process IDs on other routers. Running multiple OSPF processes on the same router is not recommended because it creates multiple database instances that add extra overhead.

Step 2 Identify which interfaces on the router are part of the OSPF process, using the **network** command. For each network, identify the OSPF area to which the network belongs. The network value is either the network address supported by the router or the specific interface addresses that are configured. The router interprets the address by comparing the address to the wildcard mask. The command is:

```
router(config-router)# network address wildcard-mask area  
area-id
```

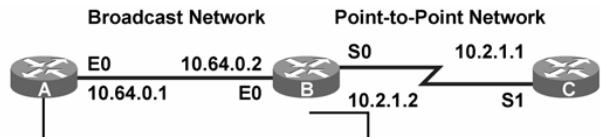
The table describes the parameters of this command.

network Parameters

Parameter	Description
<i>address</i>	Is either the network address, the subnet, or the address of the interface. This address instructs the router to recognize which links to advertise to, which links to check for advertisements, and which networks to advertise.
<i>wildcard-mask</i>	Determines how to read the address. The mask has wildcard bits, in which 0 is a match and 1 is “don’t care.” For example, 0.0.255.255 indicates a match in the first two bytes. If specifying the interface address, use the mask 0.0.0.0 to match all four bytes of the address. An address and wildcard mask combination of 0.0.0.0 255.255.255.255 matches all interfaces on the router.
<i>area-id</i>	Specifies the OSPF area to be associated with the address. This command can be a decimal number or can be in dotted-decimal notation similar to an IP address, such as A.B.C.D.

Configuring OSPF on Internal Routers of a Single Area

Cisco.com



```
<Output Omitted>
interface Ethernet0
ip address 10.64.0.1 255.255.255.0
!
<Output Omitted>
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
```

```
<Output Omitted>
interface Ethernet0
ip address 10.64.0.2 255.255.255.0
!
interface Serial0
ip address 10.2.1.2 255.255.255.0
<Output Omitted>
router ospf 50
network 10.2.1.2 0.0.0.0 area 0
network 10.64.0.2 0.0.0.0 area 0
```

Can assign network or interface address.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-5

The figure describes OSPF configuration for Ethernet broadcast networks and serial point-to-point links. All three routers in the figure are assigned to area 0 and configured for network 10.0.0.0.

Router A uses a general **network 10.0.0.0 0.255.255.255** statement. This technique assigns all interfaces defined in the 10.0.0.0 network to OSPF process 1.

Router B uses a specific host address technique. The wildcard mask of 0.0.0.0 requires a match on all four bytes of the address. This technique allows the operator to define which specific interfaces will run OSPF.

Although the two examples shown are a commonly used combination of a network statement and a wildcard mask, others could also work. For instance, a range of subnets could be specified.

The network statement and wildcard mask is not used for route summarization purposes. The network statement is used strictly to turn OSPF on for an interface or for multiple interfaces.

Verifying OSPF Operation

Cisco.com

Router#

```
show ip protocols
```

- Verifies the configured IP routing protocol processes, parameters, and statistics

Router#

```
show ip route ospf
```

- Displays all OSPF routes learned by the router

Router#

```
show ip ospf interface
```

- Displays the OSPF router ID, area ID, and adjacency information

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-6

To verify that OSPF has been properly configured, use the following **show** commands:

- The **show ip protocols** command displays IP routing protocol parameters about timers, filters, metrics, networks, and other information for the entire router.
- The **show ip route ospf** command displays the OSPF routes known to the router. 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 are configured in the intended areas. If the router does not specify a loopback address, the router chooses the interface with the highest address as the router ID. In addition, this command displays the timer intervals (including the hello interval) and shows the neighbor adjacencies.

Verifying OSPF Operation (Cont.)

Cisco.com

Router#

```
show ip ospf
```

- Displays the OSPF router ID, timers, and statistics

Router#

```
show ip ospf neighbor [detail]
```

- Displays information about the OSPF neighbors, including DR and BDR information on broadcast networks

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

- The **show ip ospf** command displays the OSPF router ID, OSPF timers, the number of times the SPF algorithm has been executed, and LSA information.
- The **show ip ospf neighbor detail** command displays a detailed list of neighbors, including their OSPF router ID, their OSPF priorities, their neighbor adjacency state (for example, init, exstart, or full), and the dead timer.

The show ip route ospf Command

Cisco.com

```
RouterA# show ip route ospf

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

Gateway of last resort is not set
      10.0.0.0 255.255.255.0 is subnetted, 2 subnets
O        10.2.1.0 [110/10] via 10.64.0.2, 00:00:50, Ethernet0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-8

Use the **show ip route ospf** command to verify the OSPF routes in the IP routing table. The O code represents OSPF routes. In the figure, the 10.2.1.0 subnet is recognized on Ethernet 0 via neighbor 10.64.0.2.

The entry “[110/10]” in the routing table represents the administrative distance assigned to OSPF (110) and the total cost of the route to subnet 10.2.1.0 (cost of 10).

The show ip ospf interface Command

Cisco.com

```
RouterA# show ip ospf interface e0

Ethernet0 is up, line protocol is up
  Internet Address 10.64.0.1/24, Area 0
  Process ID 1, Router ID 10.64.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.64.0.2, Interface address 10.64.0.2
  Backup Designated router (ID) 10.64.0.1, Interface address 10.64.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.64.0.2 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

The **show ip ospf interface** command displays OSPF-related interface information:

```
RouterA# show ip ospf interface [type number]
```

The table contains information about the parameters of this command.

show ip ospf interface Parameters

Parameter	Description
<i>type</i>	(Optional) Interface type
<i>number</i>	(Optional) Interface number

This **show ip ospf interface** command describes router A from the configuration example. The OSPF details of Ethernet interface 0 are shown in the figure. This command verifies that OSPF is running on a particular interface and gives the OSPF area that it is in.

It also displays other information, such as the OSPF process ID, the OSPF router ID, the OSPF network type, DR and BDR, timers, and neighbor adjacency.

The show ip ospf neighbor Command

Cisco.com

```
RouterB# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.64.1.1	1	FULL/BDR	00:00:31	10.64.1.1	Ethernet0
10.2.1.1	1	FULL/-	00:00:38	10.2.1.1	Serial0

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-10

The **show ip ospf neighbor** command displays OSPF neighbor information for each interface.

```
RouterB# show ip ospf neighbor [type number] [neighbor-id]  
[detail]
```

The table contains information about the parameters of this command.

show ip ospf neighbor Parameters

Parameter	Description
<i>type</i>	(Optional) Interface type
<i>number</i>	(Optional) Interface number
<i>neighbor-id</i>	(Optional) Neighbor ID
detail	(Optional) Displays a detailed list of all neighbors

One of the most important OSPF troubleshooting commands is the **show ip ospf neighbor** command. OSPF does not send or receive updates without having full adjacencies between neighbors.

In the figure, router B has two neighbors. The first entry in the table represents the adjacency formed on the Ethernet interface. A “full” state means that the LSDB has been exchanged successfully. The “BDR” entry means that this router is the backup designated router. Broadcast networks select a designated router (DR) and a BDR to help form adjacencies.

In this example, router B is the DR on the Ethernet with only one neighbor, which is the BDR. If there are other neighbors on the Ethernet, router B will have a two-way DROTHER adjacency with the other neighbors. “DROTHER” signifies a router that is not a DR or a BDR.

The second line in the table represents the neighbor of router B on the serial interface. DR and DBR are not used on point-to-point interfaces (indicated by a dash [-]).

Manipulating the OSPF Router ID

For an OSPF routing process to start successfully, it must be able to determine an OSPF router ID. This topic describes three ways to establish the OSPF router ID.

OSPF Router ID

Cisco.com

- The router is known to OSPF by the OSPF router ID number.
- LSDBs use the OSPF router ID to differentiate one router from the next.
- By default: the router ID is the highest IP address on an active interface at the moment of OSPF process startup.
- A loopback interface can override OSPF router ID. It is the highest IP address of any active loopback interface.
- An OSPF router-id command can override OSPF router ID.
- The loopback or router-id command is recommended for stability.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-11

The OSPF routing process chooses a router ID for itself when it starts up. The router ID is a unique IP address that can be assigned in the following ways:

- The highest IP address of any physical interface is chosen as the router ID. The interface does not have to be part of the OSPF process, but it has to be up. There must be at least one up IP interface on the router for OSPF to use as router ID. If no up interface with an IP address is available when the OSPF process starts, the following error message occurs:

```
p5r2(config)# router ospf 1  
2w1d: %OSPF-4-NORRID: OSPF process 1 cannot start.
```

- You should always prefer a loopback address over an interface address because a loopback address never goes down. If there is more than one loopback address, then the highest loopback address becomes the router ID.
- Using a **router-id** command is the preferred procedure to set the router ID and is always used in preference to the other two procedures.

Note The OSPF database uses the OSPF router ID to uniquely describe each router in the network. Remember that every router keeps a complete topology database of all routers and links in an area and network. The router ID should not be duplicated.

Once the OSPF router ID is set, it does not change, even if the interface that the router is using for the router ID goes down. The OSPF router ID changes only if the router reloads or if the OSPF routing process restarts.

Loopback Interfaces

Cisco.com

Unadvertised Loopback Address Ex. 192.168.255.254	Advertised Loopback Address Ex. 172.16.17.5
<ul style="list-style-type: none">• Not in OSPF table• Saves address space• Cannot use ping command	<ul style="list-style-type: none">• In OSPF table• Uses address space• Can use ping command



0452_254

Router(config)#

```
interface loopback 0
```

Router(config-if)#

```
ip address 172.16.17.5 255.255.255.255
```

- If the OSPF process is already running, the OSPF process must be cleared before the new router-id command will take effect.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

To modify the OSPF router ID to a loopback address, first define a loopback interface as follows:

```
Router(config)# interface loopback number
```

Configuring an IP address on a loopback interface overrides the highest IP address used as the router ID. OSPF is more reliable if a loopback interface is configured because the interface is always active and cannot fail, as opposed to a real interface.

For this reason, you should use the loopback address on all key routers. If the loopback address is published with the **network** command, then the other routers can ping this address for testing purposes, and a private IP address can be used to save registered public IP addresses.

Note A loopback address requires a different subnet for each router, unless the host address itself is advertised. By default, OSPF advertises loopbacks as /32 host routes.

To determine the router ID of a router, enter the **show ip ospf** command.

OSPF router-id Command

Cisco.com

```
Router(config-router)#  
router-id ip-address
```

- This command is configured under the **router ospf [process-id]** command.
- Any unique IP address can be used.
- If this command is used on an OSPF process that is already active, then the new router ID is used at the next reload or at a manual OSPF process restart using the **clear ip ospf process** command.

```
Router(config)#  
router ospf 1
```

```
Router(config-router)#  
router-id 172.16.1.1
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-13

The **router-id ospf** subordinate command is used to ensure that OSPF selects a planned router ID.

Use the following commands to ensure that OSPF selects a preconfigured router ID:

```
Router(config)# router ospf process-id  
Router(config-router)# router-id ip-address
```

After the **router-id** command is configured, use the **clear ip ospf process** command. This command restarts the OSPF routing process so that it will reselect the new IP address as its router ID.

Caution The **clear ip ospf process** command will temporarily disrupt an operational network.

OSPF Router ID Verification

Cisco.com

```
RouterA# show ip ospf

Routing Process "ospf 1" with ID 1.1.3.1
Supports only single TOS(TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Number of DCbitless external LSA 0
Number of DoNotAge external LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Area BACKBONE(0) (Active)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 10 times
    Area ranges are
      Link State Update Interval is 00:30:00 and due in 0:07:16
      Link State Age Interval is 00:20:00 and due in 00:07:15
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-14

Use the **show ip ospf** command to verify the OSPF router ID. You can also use this command to check OSPF timer settings and other statistics.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Configuration of OSPF in a single area is a two-step process:**
 - Turn on OSPF with the **router ospf** command.
 - Use the **network** statement to describe which interfaces will run OSPF.
- **OSPF configuration requires each interface to be assigned to an area number.**
- **OSPF elects a router ID at startup time using the following techniques:**
 - Highest IP address of all interfaces
 - IP address of the loopback address
 - A **router-id** command under the OSPF process

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-15

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 commands are required for basic OSPF configuration? (Choose two.)
- A) **network 0.0.0.0 255.255.255.255 area 0**
 - B) **network address wildcard-mask area area-id**
 - C) **router ospf process-id**
 - D) **ip router ospf**
- Q2) Which OSPF **show** command describes a list of OSPF adjacencies?
- A) **show ip ospf interface**
 - B) **show ip ospf**
 - C) **show ip route**
 - D) **show ip ospf neighbor**
- Q3) Which technique is NOT used for router ID selection?
- A) highest IP address on an interface
 - B) IP address on a loopback interface
 - C) lowest IP address when multiple loopback interfaces are used
 - D) the **router-id** command
- Q4) When you are using the **router-id** command, the router ID immediately changes to the IP address that has been entered.
- A) true
 - B) false

Quiz Answer Key

Q1) B, C

Relates to: Configuring Basic Single-Area OSPF

Q2) D

Relates to: Configuring Basic Single-Area OSPF

Q3) C

Relates to: Manipulating OSPF Router ID

Q4) B

Relates to: Manipulating OSPF Router ID

OSPF Network Types

Overview

This lesson describes OSPF operation in a single area by defining each OSPF network type, how the adjacencies are formed over these different OSPF network types, and how link-state advertisements LSAs are flooded on each.

It is important to note that OSPF pays special attention to different network types, such as point-to-point and broadcast networks, and that the OSPF default settings do not always work properly under some network topologies.

Relevance

Understanding that an OSPF area is made up of different types of network links is important. The adjacency behavior is different for each network type, and OSPF must be properly configured to function correctly over certain network types.

Objectives

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

- Describe adjacency behavior for a point-to-point link
- Describe adjacency behavior for a broadcast link
- Explain OSPF operations over NBMA networks
- Identify the different configuration options for OSPF over Frame Relay
- Compare common OSPF and Frame Relay configuration strategies and examples
- Interpret debug output for IP OSPF adjacencies

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Understanding of IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Adjacency Behavior for a Point-to-Point Link**
- **Adjacency Behavior for a Broadcast Network**
- **Adjacency Behavior for an NBMA Network**
- **OSPF Commands for NBMA Network Frame Relay**
- **Common OSPF Configurations for Frame Relay**
- **The debug ip ospf adj Command**
- **Summary**
- **Quiz**

Adjacency Behavior for a Point-to-Point Link

This topic describes how OSPF operates over point-to-point serial links.

Point-to-Point Links



- Usually a serial interface running either PPP or HDLC
- May also be a point-to-point subinterface running Frame Relay or ATM
- No DR or BDR election required
- OSPF autodetects this interface type
- OSPF packets are sent using multicast 224.0.0.5

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 4-4

A point-to-point network joins a single pair of routers. A T1 serial line configured with a link-layer protocol such as PPP or HDLC is an example of a point-to-point network.

On point-to-point networks, the router dynamically detects its neighboring routers by multicasting its hello packets to all SPF routers, using the address 224.0.0.5.

On point-to-point networks, neighboring routers become adjacent whenever they can communicate directly. No DR or BDR election is performed because there can be only two routers on a point-to-point link, so there is no need for a DR or BDR.

Usually, the IP source address of an OSPF packet is set to the address of the outgoing interface on the router. It is possible to use IP unnumbered interfaces with OSPF. On unnumbered interfaces, the IP source address is set to the IP address of another interface on the router.

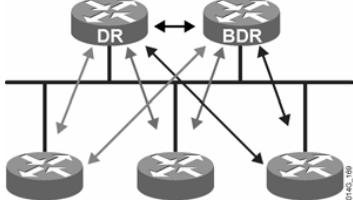
The default OSPF hello and dead intervals on point-to-point links are 10 seconds and 40 seconds, respectively.

Adjacency Behavior for a Broadcast Network

This topic describes the adjacency behavior of OSPF when it is running over broadcast network links.

Multiaccess Broadcast Network

Cisco.com



- Generally LAN technologies like Ethernet and Token Ring
- DR and BDR selection required
- All neighbor routers form full adjacencies with the DR and BDR only
- Packets to the DR and the BDR use 224.0.0.6
- Packets from DR to all other routers use 224.0.0.5

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 4-5

An adjacency is the relationship that exists between a router and its DR and BDR on a multiaccess broadcast network such as Ethernet. Adjacent routers have synchronized LSDBs. A common media segment is the basis for adjacency, for example, two routers connected on the same Ethernet segment. When routers first come up on the Ethernet, they perform the hello process and then elect the DR and BDR. The routers then attempt to form adjacencies with the DR and BDR.

The routers on a segment must elect a DR and a BDR to represent the multiaccess broadcast network. The BDR does not perform any DR functions when the DR is operating. Instead, the BDR receives all the information, but the DR performs the LSA forwarding and LSDB synchronization tasks. The BDR performs the DR tasks only if the DR fails. If the DR fails, the BDR automatically becomes the DR and a new BDR election occurs.

The DR and BDR improve network functioning in the following ways:

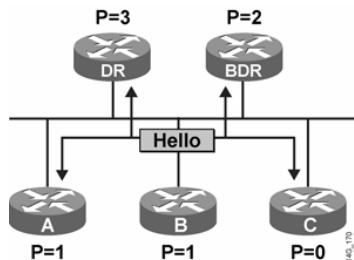
- **Reducing routing update traffic:** The DR and BDR act as a central point of contact for link-state information exchange on a multiaccess broadcast network; therefore, each router must establish a full adjacency with the DR and the BDR only. Instead of each router exchanging link-state information with every other router on the segment, each router sends the link-state information to the DR and BDR only. The DR represents the multiaccess broadcast network in the sense that it sends link-state information from each router to all other routers in the network. This flooding process significantly reduces the router-related traffic on a segment.

- **Managing link-state synchronization:** The DR and BDR ensure that the other routers on the network have the same link-state information about the internetwork. In this way, the DR and BDR reduce the number of routing errors.

Note Once a DR and BDR have been selected, any router added to the network establishes adjacencies with the DR and BDR only.

Electing the DR and BDR

Cisco.com



- Hello packets are exchanged via IP multicast.
- The router with the highest OSPF priority is selected as the DR.
- Use the OSPF router ID as the tie breaker.
- The DR election is nonpreemptive.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-6

To elect a DR and BDR, the routers view the OSPF priority value of the other routers during the hello packet exchange process and then use the following conditions to determine which router to select:

- The router with the highest priority value is the DR.
- The router with the second-highest priority value is the BDR.
- The default for the interface OSPF priority is one. In the case of a tie, the router ID is used. The router with the highest router ID becomes the DR. The router with the second-highest router ID becomes the BDR.
- A router with a priority set to zero cannot become the DR or BDR. A router that is not the DR or BDR is called a DROther.
- If a router with a higher priority value gets added to the network, it does not preempt the DR and BDR. The only time a DR or BDR changes is when one of them is out of service. If the DR is out of service, the BDR becomes the DR and a new BDR is selected. If the BDR is out of service, a new BDR is elected.

To determine whether the DR is out of service, the BDR uses the wait timer. This timer is a reliability feature. If the BDR does not confirm that the DR is forwarding LSAs before the timer expires, then the BDR assumes that the DR is out of service.

Note The highest IP address on an active interface is normally used as the router ID; however, you can override this selection by configuring an IP address on a loopback interface or using the **router-id** command.

In a multiaccess broadcast environment, each network segment has its own DR and BDR. A router connected to multiple multiaccess broadcast networks can be a DR on one segment and a regular router on another segment.

Note	Remember, the DR concept is at the link level; a DR is selected for every multiaccess broadcast link in the OSPF network.
-------------	---

Setting Priority for DR Election

Cisco.com

```
Router(config-if)#  
ip ospf priority number
```

- This interface configuration command assigns the OSPF priority to an interface.
- Different interfaces on a router may be assigned different values.
- The default priority is 1. The range is from 0 to 255.
- 0 means the router is a DROTHER; it can't be the DR or BDR.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

Use the **ip ospf priority** command to designate which router interfaces on a multiaccess link are the DR and the BDR. The interface with the highest priority becomes the DR, and the interface with the second-highest priority becomes the BDR.

Interfaces set to zero priority cannot be involved in the DR or BDR election process.

Here is a configuration example:

```
Router(config)# interface Ethernet 0  
Router(config-if)# ip ospf priority 10
```

Note The priority of an interface takes effect only when the existing DR goes down. A DR does not relinquish its status just because a new interface reports a higher priority in its hello packet.

Adjacency Behavior for an NBMA Network

This topic describes the behavior of the Hello protocol and the adjacency it forms over a nonbroadcast multiaccess (NBMA) network link.

NBMA Topology

The diagram illustrates an NBMA topology. Four router icons are arranged in a rectangle. The top-left and bottom-left routers have single lines connecting them to a central cloud. The top-right and bottom-right routers also have single lines connecting them to the same central cloud. The cloud is labeled "X.25", "Frame Relay", and "ATM". Above the cloud, there is a horizontal bar with the Cisco.com logo.

- A single interface interconnects multiple sites.
- NBMA topologies support multiple routers, but without broadcasting capabilities.
- OSPF neighbors are not automatically discovered by the router.

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 4-8

When a single interface interconnects multiple sites over a NBMA network, the nonbroadcast nature of the network can create reachability issues. NBMA networks can support more than two routers but have no broadcast capability.

For example, if the NBMA topology is not fully meshed, then a broadcast or multicast sent by one router will not reach all the other routers. Frame Relay, ATM, and X.25 are examples of NBMA networks.

To implement broadcasting or multicasting, the router replicates the packets to be broadcast or multicast and sends them individually on each permanent virtual circuit (PVC) to all destinations. This process is CPU- and bandwidth-intensive.

The default OSPF hello and dead intervals on NBMA interfaces are 30 seconds and 120 seconds, respectively.

DR Election in NBMA Topology

Cisco.com

- OSPF considers NBMA to be like other broadcast media.
- DR and BDR need to have fully meshed connectivity with all other routers, but NBMA networks are not always fully meshed.
- DR and BDR need a list of neighbors, but the NBMA interface does not automatically detect neighbors.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

OSPF considers that the NBMA environment functions in a way similar to other broadcast media such as Ethernet. However, NBMA clouds are usually built in hub-and-spoke topologies, using PVCs or switched virtual circuits (SVCs).

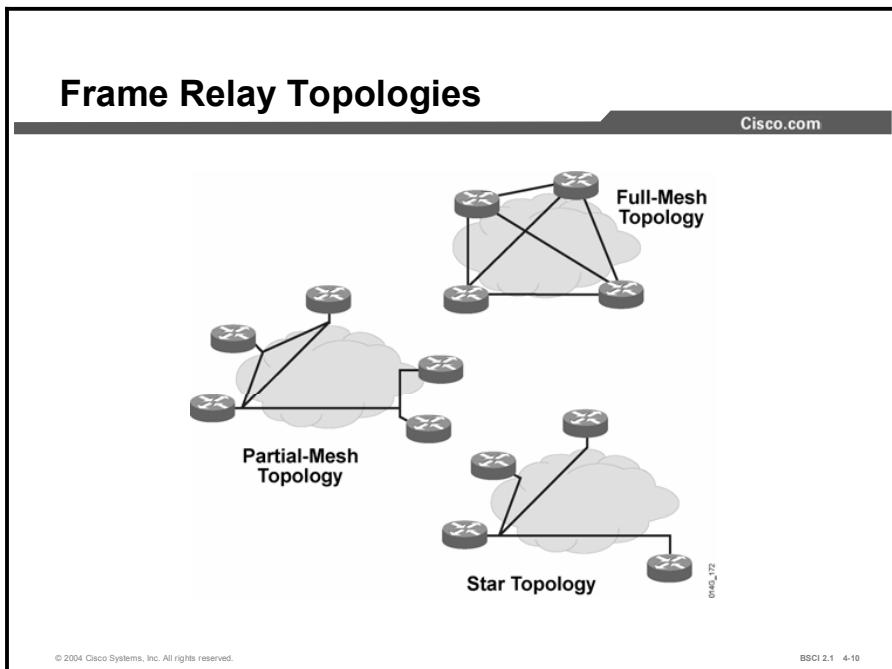
A hub-and-spoke topology means that the NBMA network is only a partial mesh. In these cases, the physical topology does not provide the multiaccess capability like Ethernet on which OSPF relies.

The election of the DR becomes an issue in NBMA topologies because the DR and BDR need to have full physical connectivity with all routers in the NBMA network. The DR and BDR also need to have a list of all the other routers so that they can establish adjacencies.

OSPF cannot automatically build adjacencies with neighboring routers over NBMA interfaces.

OSPF Commands for NBMA Network Frame Relay

There are several OSPF configuration choices for a Frame Relay network, depending on the Frame Relay network topology. This topic defines each configuration choice and explains their advantages and disadvantages.



With Frame Relay, remote sites interconnect in a variety of ways. By default, interfaces that support Frame Relay are multipoint connection types. The following examples are types of Frame Relay topologies:

- **Star topology:** A star topology, also known as a hub-and-spoke configuration, is the most common Frame Relay network topology. In this topology, remote sites connect to a central site that generally provides a service or application. The star topology is the least expensive topology because it requires the smallest number of PVCs. The central router provides a multipoint connection because it typically uses a single interface to interconnect multiple PVCs.
- **Full-mesh topology:** In a full-mesh topology, all routers have virtual circuits (VCs) to all other destinations. This method, although costly, provides direct connections from each site to all other sites and allows for redundancy. As the number of nodes in the full-mesh topology increases, the topology becomes increasingly expensive.

To figure out how many VCs are needed to implement a fully meshed topology, use the $n(n - 1) / 2$ formula, where n is the number of nodes in the network.

- **Partial-mesh topology:** In a partial-mesh topology, not all sites have direct access to a central site. This method reduces the cost of implementing a full-mesh topology.

OSPF over NBMA Topology Modes of Operation

Cisco.com

- **RFC-compliant modes are as follows:**
 - Nonbroadcast (NBMA)
 - Point-to-multipoint
- **Additional modes from Cisco are as follows:**
 - Point-to-multipoint nonbroadcast
 - Broadcast
 - Point-to-point

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-11

As described in RFC 2328, OSPF runs in one of the following two official modes in NBMA topologies:

- **Nonbroadcast:** The nonbroadcast (NBMA) mode simulates the operation of OSPF in broadcast networks. Neighbors must be manually configured, and DR and BDR election is required. This configuration is typically used with partially meshed networks.
- **Point-to-multipoint:** The point-to-multipoint mode treats the nonbroadcast network as a collection of point-to-point links. In this environment, the routers automatically identify their neighboring routers but do not elect a DR and BDR. This configuration is typically used with partially meshed networks.

The choice between NBMA and point-to-multipoint modes determines the way the Hello protocol and flooding work over the nonbroadcast network.

The main advantage of the point-to-multipoint mode is that it requires less manual configuration, and the main advantage of the nonbroadcast mode is that there is less overhead traffic..

Selecting the OSPF Network Type

Cisco.com

```
Router(config-if)#  
ip ospf network [{broadcast | nonbroadcast | point-to-  
multipoint | point-to-multipoint nonbroadcast}]
```

- This interface command defines OSPF network types.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

The **ip ospf network** interface command has several options. The table describes these options.

ip ospf network Command Options

Command Options	Description
broadcast	<ul style="list-style-type: none">■ Makes the WAN interface appear to be a LAN.■ One IP subnet.■ Uses multicast OSPF hello packet to automatically discover the neighbors.■ DR and BDR elected.■ Requires a full-mesh topology.
nonbroadcast	<ul style="list-style-type: none">■ One IP subnet.■ Neighbors must be manually configured.■ DR and BDR elected.■ DR and BDR need to have full connectivity with all other routers.■ Typically used in a partial-mesh topology.
point-to-multipoint	<ul style="list-style-type: none">■ One IP subnet.■ Uses multicast OSPF hello packet to automatically discover the neighbors.■ DR and BDR not required—router sends additional LSAs with more information about neighboring routers.■ Typically used in partial-mesh topology.
point-to-multipoint nonbroadcast	<ul style="list-style-type: none">■ If multicast and broadcast are not enabled on the VCs, the RFC-compliant point-to-multipoint mode cannot be used because the router cannot dynamically discover its neighboring routers using the hello multicast packets.■ Neighbors must be manually configured.■ DR and BDR election is not required.
point-to-point	<ul style="list-style-type: none">■ One IP subnet.■ No DR or BDR election.■ Used when only two routers need to form an adjacency on a pair of interfaces.■ Interfaces can be either LAN or WAN.

Example

The following is a sample configuration of a Frame Relay router in a full-mesh topology, with the broadcast mode of operation defined:

```
Interface serial 0
  Encapsulation frame-relay
  Ip ospf network broadcast
```

Common OSPF Configurations for Frame Relay

This topic explains the concept and configuration of each of the common OSPF over Frame Relay modes of operation.

Nonbroadcast Mode (NBMA Mode)

Cisco.com

- Treated as a broadcast network by OSPF (acts like a LAN)
- All serial ports are part of the same IP subnet
- Frame Relay, X.25, and ATM networks default to NBMA operation
- Neighbors must be statically configured
- Duplicates LSA updates
- RFC 2328-compliant

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-13

In nonbroadcast mode, OSPF emulates operation over a broadcast network. A DR and BDR are elected for the NBMA network, and the DR originates an LSA for the network. In this environment, the routers are usually fully meshed to facilitate the establishment of adjacencies among the routers.

If the routers are not fully meshed, then you should select the DR and BDR manually to ensure that the selected DR and BDR have full connectivity to all other neighboring routers. Neighboring routers are statically defined to start the DR and BDR election process. When using nonbroadcast mode, all routers are on one IP subnet.

For flooding over a nonbroadcast interface, the LSU packet must be replicated for each PVC. The updates are sent to each of the neighboring routers defined in the neighbor table on the interface.

When there are few neighbors in the network, nonbroadcast mode is the most efficient way to run OSPF over NBMA networks because it has less overhead than the point-to-multipoint mode.

Using the neighbor Command

Cisco.com

```
Router(config-router)#
neighbor x.x.x.x [priority number]
[poll-interval number]
```

- Router OSPF subordinate command
- Used to statically define neighbor relationships in an NBMA network

©2004 Cisco Systems, Inc. All rights reserved.

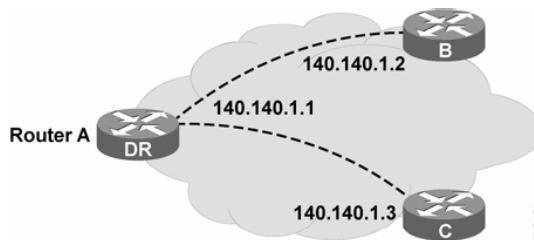
BSCI 2.1 4-14

The **neighbor** command is used to statically define adjacent relationships in NBMA networks using the nonbroadcast mode. The **neighbor** command has the options shown in the table.

Command	Description
x.x.x.x	IP address of the neighboring router.
priority number	Specifies priority with priority number; zero means neighboring router does not become DR.
poll-interval number	Amount of time an NBMA interface waits before sending hellos to the neighbor even if the neighbor is inactive. The poll interval is defined in seconds.

neighbor Command Example

Cisco.com



```
RouterA(config)# router ospf 100
RouterA(config-router)# network 140.140.0.0 0.0.255.255 area 0
RouterA(config-router)# neighbor 140.140.1.2 priority 0
RouterA(config-router)# neighbor 140.140.1.3 priority 0
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-15

This figure exemplifies statically defining adjacencies. All three routers are using the nonbroadcast mode on their Frame Relay interfaces; therefore, each must manually configure its neighboring routers.

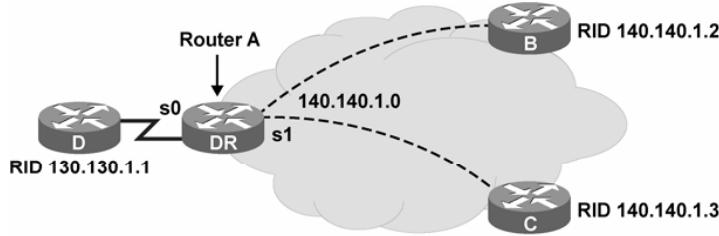
The **priority** command should be set to 0 for routers B and C because a full-mesh topology does not exist. This configuration ensures that router A becomes the DR because only router A has full connectivity to the other two routers. No BDR will be elected in this case.

In an NBMA network, **neighbor** statements are required only on the DR and BDR. In a hub-and-spoke topology, **neighbor** statements must be used for the hub, which must additionally be configured to become the DR.

Neighbor statements are not mandatory on the spoke routers. In a full-mesh NBMA topology, you may need **neighbor** statements on all routers unless you have statically configured the DR and BDR using the **priority** command.

The show ip ospf neighbor Command

Cisco.com



RouterA# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
130.130.1.1	1	full/-	0:00:35	128.12.1.2	s0
201.23.13.1	0	full/drother	0:00:36	140.140.1.2	s1
192.100.1.1	0	full/drother	0:00:34	140.140.1.3	s1

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-16

The following command displays OSPF neighbor information on a per-interface basis:

```
RouterA# show ip ospf neighbor [type number] [neighbor-id] [detail]
```

The table lists and describes the parameters of the **show ip ospf neighbor** command.

show ip ospf neighbor Parameters

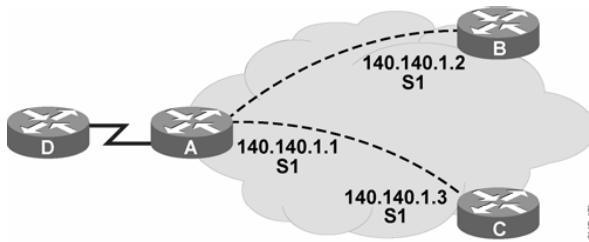
Parameter	Description
type	(Optional) Interface type
number	(Optional) Interface number
neighbor-id	(Optional) ID for neighboring router
detail	(Optional) Displays a detailed list of all neighboring routers

The figure shows a router with two serial interfaces; serial 0 is a point-to-point interface, and serial 1 is a Frame Relay NBMA interface. The neighbor learned for serial 0 has a state of “full/-,” which means that it has successfully exchanged LSDB information with the router issuing the **show** command, and that no DR or BDR is required on a point-to-point network.

The serial 1 interface on this router shows two neighbors; both have a state of “full/drother.”

Point-to-Multipoint Mode

Cisco.com



- The point-to-multipoint mode allows for NBMA networking.
- The point-to-multipoint mode fixes partial-mesh and star topologies.
- No DR is required and only a single subnet is used.
- A 30-second hello is used.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-17

Networks in point-to-multipoint mode are designed to work with partial-mesh or star topologies. In point-to-multipoint mode, OSPF treats all router-to-router connections over the nonbroadcast network as if they were point-to-point links. In the point-to-multipoint mode, DRs are not used, and a type 2 network LSA is not flooded to adjacent routers. Instead, OSPF point-to-multipoint works by exchanging additional LSUs that are designed to automatically discover neighboring routers and add them to the neighbor table.

In large networks, using point-to-multipoint mode reduces the number of PVCs required for complete connectivity because you are not required to have a full-mesh topology. In addition, not having a full-mesh topology reduces the number of neighbor entries in the neighbor table. Point-to-multipoint mode has the following properties:

- **Does not require a fully meshed network:** This environment allows routing to occur between two routers that are not directly connected but are connected through a router that has VCs to each of the two routers. All three routers in the figure can be configured for point-to-multipoint. The point-to-multipoint and the nonbroadcast modes use a 30-second hello timer, while the point-to-point mode uses a 10-second hello timer. The hello and dead timers on the neighboring interfaces must match in order for the neighbors to form successful adjacencies.
- **Does not require a static neighbor configuration:** In nonbroadcast (NBMA) mode, neighboring routers are statically defined to start the DR election process and allow the exchange of routing updates. However, because the point-to-multipoint mode treats the network as a collection of point-to-point links, multicast hello packets discover neighboring routers dynamically. Statically configuring neighboring routers is not necessary.
- **Uses one IP subnet:** As in nonbroadcast (NBMA) mode, when you are using point-to-multipoint mode, all routers are on one IP subnet.
- **Duplicates LSA packets:** Also as in nonbroadcast (NBMA) mode, when you are flooding a nonbroadcast interface in point-to-multipoint mode, the router must replicate the LSU. The LSU packet is sent to each of the neighboring routers defined in the neighbor table of the interface.

Point-to-Multipoint Configuration

Cisco.com

```
RouterA(config)# interface serial 0
RouterA(config-if)# encapsulation hdlc
RouterA(config-if)# ip address 120.120.1.1 255.255.255.0
RouterA(config)# interface serial 1
RouterA(config-if)# encapsulation frame-relay
RouterA(config-if)# ip address 140.140.1.1 255.255.255.0
RouterA(config-if)# ip ospf network point-to-multipoint
```

```
RouterB(config)# interface serial 0
RouterB(config-if)# ip address 140.140.1.2 255.255.255.0
RouterB(config-if)# encapsulation frame-relay
RouterB(config-if)# ip ospf network point-to-multipoint
```

- Frame Relay Inverse ARP enabled (default)

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-18

This figure shows partial configurations from the point-to-multipoint example of routers A and B. This configuration does not require subinterfaces and uses only a single subnet. In point-to-multipoint mode, a DR or BDR is not required; therefore, DR and BDR election and priorities are not a concern.

Point-to-Multipoint Example

Cisco.com

```
RouterA# show ip ospf interface s1
Serial1 is up, line protocol is up
  Internet Address 140.140.1.1/24, Area 1
  Process ID 100, Router ID 120.120.1.1, Network Type Point-To-Multipoint,
Cost: 64
  Transmit Delay is 1 sec, State: Point To Multipoint
  Timer intervals configured,Hello 30, Dead 120, Wait 120, Retransmit 5
  Hello due in 00:00:11
  Neighbor count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 140.140.1.2
  Adjacent with neighbor 140.140.1.3
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-19

The **show ip ospf interface** command displays key OSPF details for each interface.

The OSPF network type, area number, cost, and state of the interface are all displayed. The hello interval for a point-to-multipoint interface is 30 seconds, with a dead interval of 120 seconds.

The listed adjacent neighboring routers are all dynamically learned. Manual configuration of neighboring routers is not necessary.

Point-to-Multipoint Nonbroadcast

Cisco.com

- Cisco extension to point-to-multipoint RFC
- Must statically define neighbors, like normal NBMA
- Like point-to-multipoint mode, DR not elected
- Used in special cases where neighbors cannot be automatically discovered

RouterA(config-if)#

```
ip ospf network point-to-multipoint [nonbroadcast]
```

- Defines a special version of the point-to-multipoint mode; note the nonbroadcast option

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-20

Cisco defines additional modes for the OSPF neighbor relationship. Following is a description of these modes:

- **Point-to-multipoint nonbroadcast:** This mode is a Cisco extension of the RFC-compliant point-to-multipoint mode. You must statically define neighbors, and you can modify the cost of the link to the neighboring router to reflect the different bandwidths of each link. The RFC point-to-multipoint mode was developed to support underlying point-to-multipoint VCs that support multicast and broadcast; therefore, this mode allows dynamic neighboring router discovery. If multicast and broadcast are not enabled on the VCs, the RFC-compliant point-to-multipoint mode cannot be used because the router cannot dynamically discover its neighboring routers using the hello multicast packets.
- **Broadcast:** This mode is a workaround for statically listing all existing neighboring routers. The interface is set to broadcast and behaves as though the router connects to a LAN. DR and BDR election is still performed; therefore, take special care to ensure either a full-mesh topology or a static election of the DR based on the interface priority.
- **Point-to-point:** This mode is used when only two nodes exist on the NBMA network. The point-to-point mode is typically used only with point-to-point subinterfaces. Each point-to-point connection is one IP subnet. An adjacency forms over the point-to-point network with no DR or BDR election.

Using Subinterfaces

Cisco.com

Router(config)#

```
interface serial 0.[x] point-to-point
```

- This is a global configuration command. The subinterface number is x.
- The physical serial port becomes multiple logical ports.
- Each PVC and SVC gets its own subinterface.
- Limitations:
 - Each subinterface requires an IP subnet.
 - Hello and LSA packets are multiplied by the number of subinterfaces. Hellos are sent every 10 seconds.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-21

A physical interface can be split into multiple logical interfaces, called subinterfaces. Each subinterface is defined as a point-to-point or a point-to-multipoint interface. Subinterfaces were originally created to better handle issues caused by split horizon over NBMA for distance vector-based routing protocols. A point-to-point subinterface has the properties of any physical point-to-point interface.

Define subinterfaces using the following command:

```
Router(config)# interface serial number.subinterface-number  
{multipoint | point-to-point}
```

The table lists the parameters of the **interface serial** command.

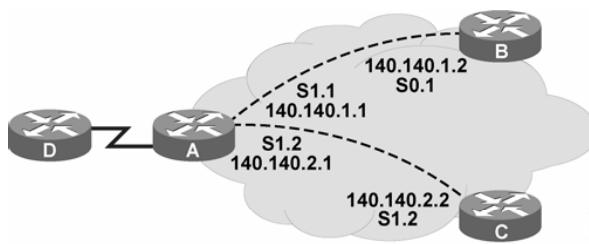
interface serial Parameters

Parameter	Description
number.subinterface-number	<ul style="list-style-type: none">■ Interface number and subinterface number.■ Subinterface number is in the range of 1 to 4294967293.■ Interface number that precedes the period (.) must match the interface number to which this subinterface belongs.
multipoint	<ul style="list-style-type: none">■ On multipoint subinterfaces routing IP, all routers are in the same subnet.
point-to-point	<ul style="list-style-type: none">■ On point-to-point subinterfaces routing IP, each pair of point-to-point routers is in its own subnet.

The default OSPF mode on a point-to-point Frame Relay subinterface is the point-to-point mode; the default OSPF mode on a Frame Relay point-to-multipoint subinterface is the nonbroadcast mode. The default OSPF mode on a main Frame Relay interface is also the nonbroadcast mode.

Subinterface Example

Cisco.com



- PVCs on the right are treated like the point-to-point link on the left.
- Each subinterface requires a subnet.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-22

Although all three routers have only one physical serial port, router A appears to have two logical ports. Each logical port (subinterface) has its own IP address and operates as point-to-point OSPF network type.

Each subinterface is on its own IP subnet. This type of configuration avoids the need for a DR or BDR and removes the requirement to statically define the neighbors.

Multipoint Subinterfaces

Cisco.com

Router(config)#

```
interface serial 0.x multipoint
```

- This is a global configuration command.
The subinterface number is x.
- The physical serial port becomes multiple logical ports.
- Multiple PVCs are on a single subinterface.
- NBMA mode is the default for multipoint subinterfaces.
- Limitations:
 - Each subinterface requires an IP subnet.
 - Hello and LSA packets are multiplied by the number of subinterfaces. Hellos are sent every 10 seconds.

© 2004 Cisco Systems, Inc. All rights reserved.

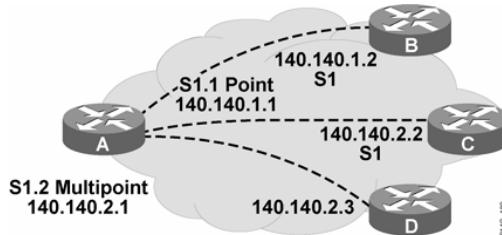
BSCI 2.1 4-23

Multipoint Frame Relay subinterfaces default to the nonbroadcast OSPF network type. The nonbroadcast OSPF network type requires neighbors to be statically configured, and DR and BDR election is required.

During the configuration of subinterfaces, you must choose the **point-to-point** or **multipoint** keywords. The choice of modes affects the operation of OSPF.

Multipoint Subinterface Example

Cisco.com



- Single interface serial 1 has been logically separated by two subinterfaces: one point-to-point and one multipoint.
- Each subinterface requires a subnet.
- OSPF defaults to NBMA mode on multipoint subinterfaces.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-24

In this figure, router A has one subinterface using point-to-point mode and a second subinterface using multipoint. The multipoint subinterface supports two other routers in a single subnet. OSPF treats the multipoint interface as NBMA by default.

OSPF treats the point-to-point subinterface as a point-to-point OSPF network type by default.

OSPF treats the multipoint interface as a nonbroadcast OSPF network type by default.

OSPF over NBMA Topology Summary

Cisco.com

OSPF Mode	NBMA Preferred Topology	Subnet Address	Hello Timer	Adjacency	RFC or Cisco
Nonbroadcast (NBMA)	Fully Meshed	Same	30 sec	Manual Configuration DR/BDR Elected	RFC
Broadcast	Fully Meshed	Same	10 sec	Automatic DR/BDR Elected	Cisco
Point-to-Multipoint	Partial-Mesh or Star	Same	30 sec	Automatic No DR/BDR	RFC
Point-to-Multipoint Nonbroadcast	Partial-Mesh or Star	Same	30 sec	Manual Configuration No DR/BDR	Cisco
Point-to-Point	Partial-Mesh or Star, Using Subinterface	Different for Each Subinterface	10 sec	Automatic No DR/BDR	Cisco

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-25

01452190

The figure provides a concise comparison of the various modes of operation for OSPF over NBMA topologies.

The debug ip ospf adj Command

Understanding OSPF adjacency protocol handshakes is important in troubleshooting. This topic describes the **debug** command, used for troubleshooting.

Creation of Adjacencies

Cisco.com

```
Router# debug ip ospf adj

Point-to-point interfaces coming up: No election
%LINK-3-UPDOWN: Interface Serial1, changed state to up
OSPF: Interface Serial1 going Up
OSPF: Rcv hello from 192.168.0.11 area 0 from Serial1 10.1.1.2
OSPF: End of hello processing
OSPF: Build router LSA for area 0, router ID 192.168.0.10
OSPF: Rcv DBD from 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x7 len 32
state INIT
OSPF: 2 Way Communication to 192.168.0.11 on Serial1, state 2WAY
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x167F opt 0x2 flag 0x7 len 32
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x2 len 72
```

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 4-26

Use the **debug ip ospf adj** command to track OSPF adjacencies as they come up or go down. Debugging allows you to see exactly which OSPF packets are being sent between routers. The ability to see packets as they are sent over a link is an invaluable tool to the troubleshooter.

In the figure, the partial **debug** output from the **debug** command describes a serial interface in point-to-point mode. No DR election occurs; however, the adjacency forms, allowing database description (DBD) packets to be sent during the exchange process.

Notice that the neighbor relationship passes through the two-way phase and into the exchange phase. Once DBD packets are sent between routers, the neighbors move into the final state: full adjacency.

Creation of Adjacencies (Cont.)

Cisco.com

```
RouterA# debug ip ospf adj

Ethernet interface coming up: Election
OSPF: 2 Way Communication to 192.168.0.10 on Ethernet0, state 2WAY
OSPF: end of Wait on interface Ethernet0
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.12
OSPF: Elect DR 192.168.0.12
    DR: 192.168.0.12 (Id)   BDR: 192.168.0.12 (Id)
OSPF: Send DBD to 192.168.0.12 on Ethernet0 seq 0x546 opt 0x2 flag 0x7 len 32
<...>
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.11
OSPF: Elect DR 192.168.0.12
    DR: 192.168.0.12 (Id)   BDR: 192.168.0.11 (Id)
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-27

The figure shows a partial **debug ip ospf adj** output illustrating the DR and BDR election process on an Ethernet interface. The OSPF default behavior on an Ethernet link is broadcast mode. First, the DR and BDR are selected, and then the exchange process occurs.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **OSPF defines a variety of network types:**
 - Point-to-point (example is a T1 serial interface)
 - Broadcast (example is a LAN interface like Ethernet)
 - Nonbroadcast (NBMA) (example is Frame Relay configured on a serial interface)
 - Point-to-multipoint (example is OSPF over Frame Relay mode that eliminates the need for a DR)
 - Point-to-multipoint nonbroadcast (Cisco specific)
- **Each mode of operation has advantages and disadvantages. A network operator must understand each option and make the proper configuration choices.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-28

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 4-1: Configuring and Examining OSPF in a Single Area

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) OSPF does not require a Hello protocol on point-to-point links because the adjacent router is directly connected.
- A) true
 - B) false
- Q2) Three routers are connected to an Ethernet LAN. One is a small router that should not take on the role of DR or BDR. How do you ensure that it never will?
- A) Set the interface priority to 100.
 - B) Set the interface priority to 0.
 - C) Leave the interface priority set to 1 and set the priority of the other two routers to 10.
 - D) Use the **no designated-router** command on the Ethernet interface.
- Q3) When the DR fails, the BDR builds new adjacencies, exchanges databases, and takes over as DR automatically.
- A) true
 - B) false
- Q4) What is the hello interval for NBMA interfaces?
- A) 10 seconds
 - B) 30 seconds
 - C) 120 seconds
 - D) 60 seconds
- Q5) An OSPF automatically builds adjacencies with neighboring routers on an NBMA link.
- A) true
 - B) false
- Q6) Which mode of OSPF operation is RFC-compliant?
- A) point-to-multipoint nonbroadcast
 - B) point-to-multipoint
 - C) broadcast
 - D) point-to-point

- Q7) Match the Frame Relay or OSPF mode of operation with its description.
- A) broadcast
B) point-to-multipoint
C) nonbroadcast (NBMA)
- _____ 1. does not discover neighbor list automatically
_____ 2. generally requires a full Frame Relay mesh
_____ 3. used in partial-mesh topologies, does not require DR and BDR election, automatically discovers neighbors
- Q8) Which two OSPF over Frame Relay modes elect a DR? (Choose two.)
- A) broadcast
B) nonbroadcast
C) point-to-multipoint
D) point-to-point
- Q9) A point-to-point subinterface solves which two problems with OSPF over Frame Relay? (Choose two.)
- A) works with multiple vendors
B) manual configuration of neighbors not required
C) DR and BDR not required
D) saves on subnets
- Q10) When troubleshooting a DR election problem, which is an excellent command to use?
- A) **show ip ospf**
B) **show ip route**
C) **debug ip ospf neighbor**
D) **debug ip ospf adj**

Quiz Answer Key

- Q1) B
Relates to: Adjacency Behavior for a Point-to-Point Link
- Q2) B
Relates to: Adjacency Behavior for a Broadcast Network
- Q3) B
Relates to: Adjacency Behavior for a Broadcast Network
- Q4) B
Relates to: Adjacency Behavior for an NBMA Network
- Q5) B
Relates to: Adjacency Behavior for an NBMA Network
- Q6) B
Relates to: OSPF Commands for NBMA Frame Relay
- Q7) 1-C, 2-A, 3-B
Relates to: OSPF Commands for NBMA Frame Relay
- Q8) A, D
Relates to: Common OSPF Configurations for Frame Relay
- Q9) A, C
Relates to: Common OSPF Configurations for Frame Relay
- Q10) D
Relates to: The debug ip ospf adj Command

Types of OSPF Routers and Link-State Advertisements

Overview

The two core concepts of OSPF are the link-state database (LSDB) and link-state advertisements (LSAs). This lesson describes each of the common LSA types and how they form the layout of the OSPF LSDB. This lesson also describes OSPF router types, area border routers (ABRs), Autonomous System Boundary Routers (ASBRs), and internal routers.

Relevance

There is nothing more important in OSPF than understanding how the topology database is built. Troubleshooting OSPF often requires analyzing the OSPF database and routing table; therefore, a solid understanding of the OSPF database and LSAs is essential.

Objectives

Upon completing this lesson, you will be able to meet the following objectives:

- List the types of OSPF routers
- Explain, in general terms, all the LSAs defined by OSPF and specifically describe the most common LSAs used in OSPF today
- Interpret the OSPF LSDB and routing table

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Familiarity with IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

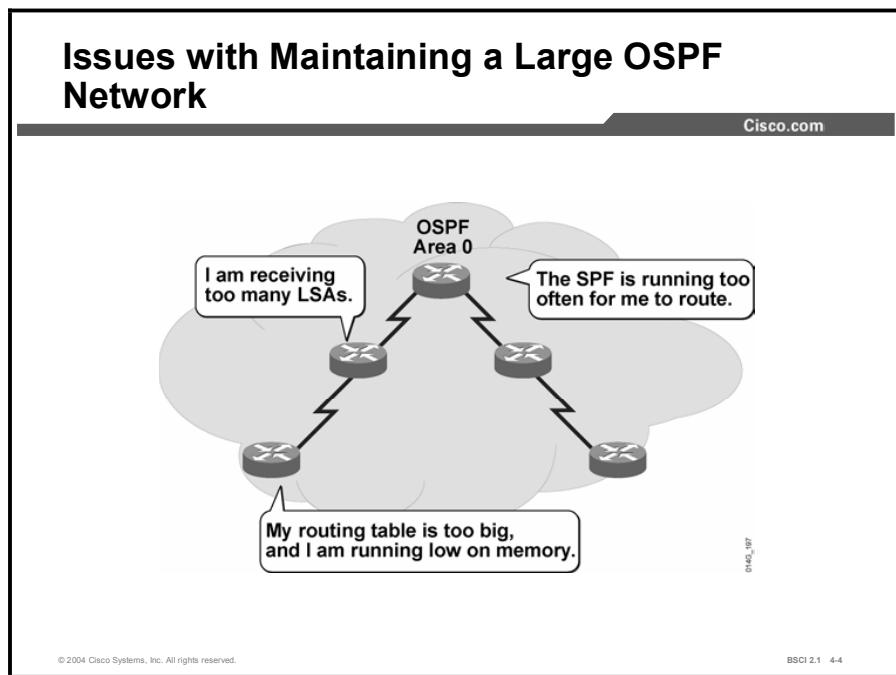
Outline

Cisco.com

- **Overview**
- **Types of OSPF Routers**
- **OSPF LSA Types**
- **Interpreting the OSPF LSDB and Routing Table**
- **Summary**
- **Quiz**

Types of OSPF Routers

The OSPF LSDBs are often very large. For this reason, an area hierarchical structure has been imposed that defines several router types. This topic defines the following router types: internal, backbone, ABR, and ASBR.



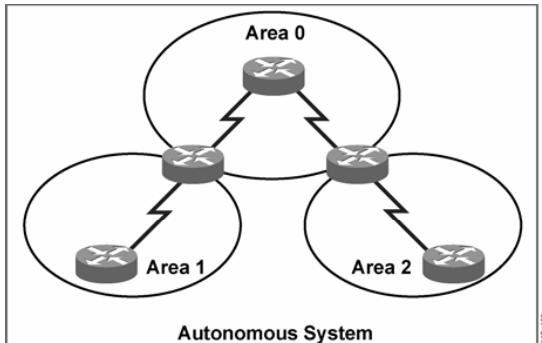
OSPF usually operates within a single area; however, certain issues arise if this single area expands into hundreds of networks. If an expansion occurs, the following issues need to be addressed:

- **Frequent SPF algorithm calculations:** In a large network, changes are inevitable; therefore, the routers spend many CPU cycles recalculating the SPF algorithm and updating the routing table.
- **Large routing table:** OSPF does not perform route summarization by default. If the routes are not summarized, the routing table can become very large, depending on the size of the network.
- **Large LSDB:** Because the LSDB covers the topology of the entire network, each router must maintain an entry for every network in the area, even if all routes are not selected for the routing table.

A solution to these issues is to divide the network into multiple OSPF areas. OSPF allows the separation of a large area into smaller, more manageable areas that are still able to exchange routing information.

The Solution: OSPF Hierarchical Routing

Cisco.com



- **Consists of areas and autonomous systems**
- **Minimizes routing update traffic**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-5

Hierarchical area routing is the ability of OSPF to separate a large internetwork into multiple areas. When you use this technique, interarea routing still occurs, but many of the internal routing operations, such as SPF calculations, remain within individual areas.

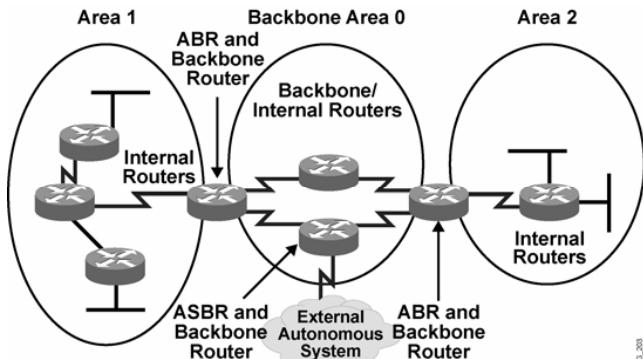
For example, if area 1 is having problems with a link going up and down, routers in other areas do not need to continually run their SPF calculation, because they are isolated from the problem in area 1.

Using multiple OSPF areas has several important advantages:

- **Reduced frequency of SPF calculations:** Because detailed route information exists within each area, it is not necessary to flood all link-state changes to all other areas. Therefore, only the routers that are affected by the change need to recalculate SPF.
- **Smaller routing tables:** With multiple areas, detailed route entries for specific networks within an area remain in the area. Instead of advertising these explicit routes outside the area, routers can be configured to summarize the routes into one or more summary addresses. Advertising these summaries reduces the number of LSAs propagated between areas but keeps all networks reachable.
- **Reduced LSU overhead:** LSUs contain a variety of LSA types, including link-state and summary information. Rather than send an LSU about each network within an area, a router can advertise a single summarized route or small number of routes between areas, reducing the overhead associated with LSUs when they cross areas.

Types of OSPF Routers

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-10

Certain types of OSPF routers control the traffic types that go in and out of various areas. Following are the four router types:

- **Internal routers:** Routers that have all their interfaces in the same area and have identical LSDBs.
- **Backbone routers:** Routers that sit in the perimeter of the backbone area and have at least one interface connected to area 0. Backbone routers maintain OSPF routing information using the same procedures and algorithms as internal routers.
- **ABRs:** Routers that have interfaces attached to multiple areas, maintain separate LSDBs for each area to which they connect, and route traffic destined for or arriving from other areas. ABRs are exit points for the area, which means that routing information destined for another area can get there only via the ABR of the local area.
ABRs can be configured to summarize the routing information from the LSDBs of their attached areas. ABRs distribute the routing information into the backbone. The backbone routers then forward the information to the other ABRs. An area can have one ABR or more.
- **ASBRs:** Routers that have at least one interface attached to an external internetwork (another autonomous system), such as a non-OSPF network. ASBRs can import non-OSPF network information to the OSPF network and vice versa; this process is called route redistribution.

A router can exist as more than one router type. For example, if a router interconnects to area 0 and area 1, as well as to a non-OSPF network, it is both an ABR and an ASBR.

A router has a separate LSDB for each area to which it connects. Therefore, an ABR could have one LSDB for area 0 and another LSDB for another area in which it participates. Two routers belonging to the same area maintain identical LSDBs for that area.

An LSDB is synchronized between pairs of adjacent routers. On broadcast networks like Ethernet, an LSDB is synchronized between the DRother and its DR and BDR.

OSPF LSA Types

LSAs are the building blocks of the OSPF LSDB. Individually, they act as database records; in combination, they describe the entire topology of an OSPF network or area. This topic first lists the LSAs defined in OSPF and then describes in detail the LSAs that are most commonly used.

The screenshot shows a table titled "LSA Types" with the following data:

LSA Type	Description
1	Router Link Advertisements
2	Network Link Advertisements
3 or 4	Summary Link Advertisements
5	Autonomous System External Link Advertisements
6	Multicast OSPF LSA
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9, 10, 11	Opaque LSAs

Type 1

Every router generates router link advertisements for each area to which it belongs. Router link advertisements describe the state of the links of the router to the area and are flooded only within a particular area. For all types of LSAs, there are 20-byte LSA headers. One of the fields of the LSA header is the link-state ID. The link-state ID of the type 1 LSA is the originating ID of the router.

Type 2

DRs generate network link advertisements for multiaccess networks that describe the set of routers attached to a particular multiaccess network. Network link advertisements are flooded in the area that contains the network. The link-state ID of the type 2 LSA is the IP interface address of the DR.

Types 3 and 4

ABRs generate summary link advertisements. Summary link advertisements describe the following interarea routes:

- Type 3 describes routes to networks and aggregates routes
- Type 4 describes routes to ASBRs

Link-state ID is the destination network number for type 3 LSAs and the router ID of the described ASBR for type 4 LSAs.

These LSAs are flooded throughout the backbone area to the other ABRs. These link entries are not flooded into the totally stubby area.

Type 5

ASBRs generate autonomous system external link advertisements. External link advertisements describe routes to destinations external to the autonomous system and are flooded everywhere with the exception of stub areas. The link-state ID of the type 2 LSA is the external network number.

Type 6

Type 6 LSAs are specialized LSAs used in multicast OSPF applications.

Type 7

Type 7 is an LSA type used in a special area known as a not-so-stubby area (NSSA).

Type 8

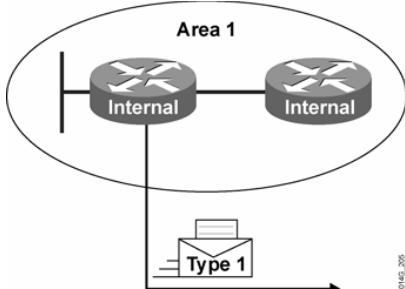
Type 8 is a specialized LSA used in internetworking OSPF and Border Gateway Protocol (BGP).

Types 9, 10, and 11

These LSA types are designated for future upgrades to OSPF. The opaque LSAs are types 9, 10, and 11, which are used for application-specific purposes. For example, Cisco uses opaque LSAs for Multiprotocol Label Switching (MPLS) with OSPF. Standard LSDB flooding mechanisms are used for distribution of opaque LSAs. Each of the three types has a different flooding scope.

LSA Type 1: Router LSA

Cisco.com



- One router LSA for every router in an area
 - Includes list of directly attached links
 - Each link identified by IP prefix assigned to link
- Identified by the router ID of the originating router
- Floods within its area only, does not cross ABR

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

A router advertises a type 1 LSA that floods to all other routers in the area from where it originated. Type 1 LSA describes the collective states of the directly connected links (interfaces) of the router.

The router ID identifies each type 1 LSA. The LSA describes each link by the network number and mask of the specific link, known as the link ID. In addition, the type 1 LSA describes whether the router is an ABR or ASBR.

Type 1 LSA links are described in the table.

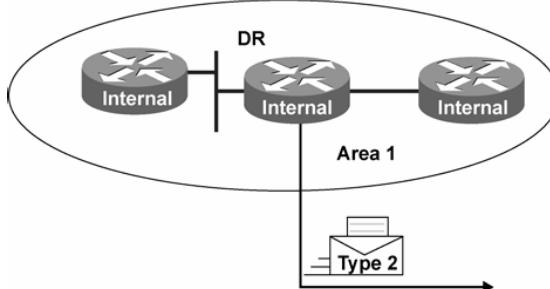
LSA Type 1 Links

Link Type	Description	Link ID
1	Point-to-point	Neighboring router ID
2	Transit network	Interface address of DR
3	Stub network	IP network number
4	Virtual link	Neighboring router ID

A stub network is a dead-end link that has only one router attached. A virtual link is a special case in OSPF.

LSA Type 2: Network LSA

Cisco.com



- **One network (type 2) LSA for each transit broadcast or NBMA network in an area**
 - Includes list of attached routers on the transit link
 - Includes subnet mask of link
- **Advertised by the DR of the broadcast network**
- **Floods within its area only, does not cross ABR**

© 2004 Cisco Systems, Inc. All rights reserved.

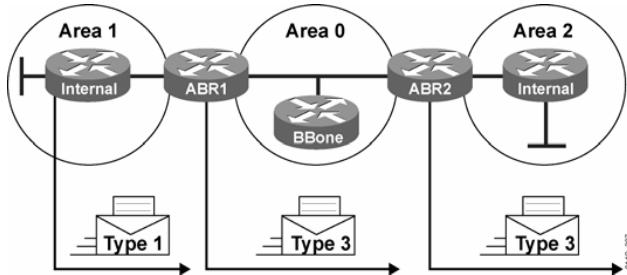
BSCI 2.1 4-13

A type 2 LSA is generated for every transit network within an area. A transit network has at least two directly attached OSPF routers. A multiaccess network like Ethernet is an example of a transit network. A type 2 network LSA lists each of the attached routers that make up the transit network.

The DR of the transit link is responsible for advertising the network LSA. The type 2 LSA then floods to all routers within the transit network area. Type 2 LSAs never cross an area boundary. The LSA ID for a network LSA is the IP interface address of the DR that advertises it.

LSA Type 3: Summary LSA

Cisco.com



- Used to flood network information to areas outside the originating area (interarea).
 - Describes network number and mask of link
- Advertised by the ABR of originating area.
- Flood throughout the autonomous system.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-14

The ABR sends type 3 summary LSAs. A type 3 LSA advertises any networks owned by an area to the rest of the areas in the OSPF autonomous system.

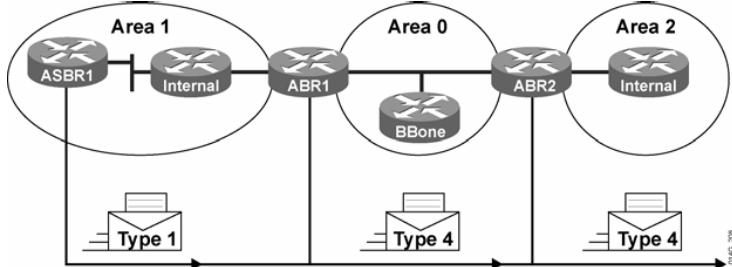
By default, OSPF does not automatically summarize groups of contiguous subnets, or even summarize a network to its classful boundary. The network operator, through configuration commands, must specify how the summarization will occur.

Therefore, by default, a type 3 LSA is advertised into the backbone area for every subnet defined in the originating area, which can cause significant flooding problems.

Consequently, you should always consider using manual route summarization at the ABR.

LSA Type 4: Summary LSA

Cisco.com



- Summary (type 4) LSAs are used to advertise an ASBR to all other areas in the autonomous system.
- They are generated by the ABR of the originating area.
- Type 4 LSAs flood throughout the autonomous system.
- They are regenerated by all subsequent ABRs.
- Type 4 LSA contains the router ID of the ASBR only.

©2004 Cisco Systems, Inc. All rights reserved.

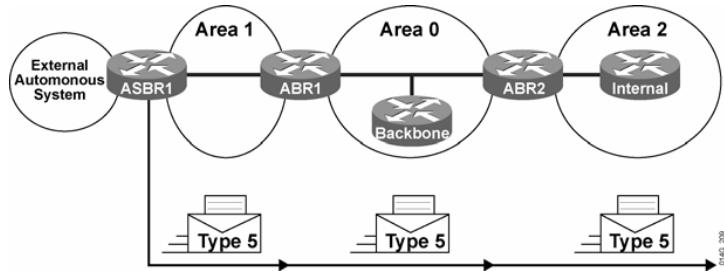
BSCI 2.1 4-15

A type 4 summary LSA is used only when an ASBR exists within an area. A type 4 LSA identifies any ASBR and provides a route to it. All traffic destined to an external autonomous system requires routing table knowledge of the ASBR that originated the external routes.

In the figure, the ASBR sends a type 1 router LSA with a bit (known as the E [external] bit) that is set to identify itself as an ASBR. When the ABR (identified with the B [border] bit in the router LSA) receives this type 1 LSA, it builds a type 4 LSA and floods it to the backbone, area 0.

LSA Type 5: External LSA

Cisco.com



- External (type 5) LSAs are used to advertise networks from other autonomous systems.
- Type 5 LSAs are advertised and owned by the originating ASBR.
- Type 5 LSAs flood throughout the entire autonomous system.
- The advertising router ID ASBR is unchanged throughout the autonomous system.
- Type 4 LSA is needed to find the ASBR.

©2004 Cisco Systems, Inc. All rights reserved.

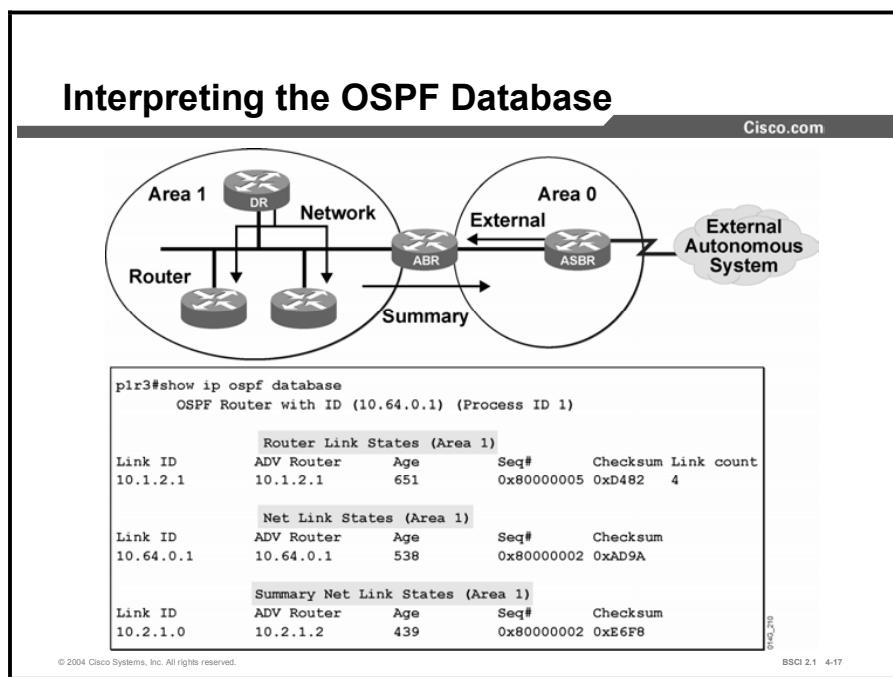
BSCI 2.1 4-16

Type 5 external LSAs describe routes to networks outside the OSPF autonomous system. Type 5 LSAs are originated by the ASBR and are flooded to the entire autonomous system. Because of the flooding scope and depending on the number of external networks, lack of route summarization can also be a major issue with external LSAs.

You should always attempt to summarize blocks of external network numbers at the ASBR to reduce flooding problems.

Interpreting the OSPF LSDB and Routing Table

OSPF LSDB and the IP routing table are two of the most important concepts to understand for OSPF operation. This topic details the **show ip ospf database** and the **show ip route** commands.



The figure illustrates use of the **show ip ospf database** command to get information about an OSPF LSDB. The router link states are type 1 LSAs, the net link states are type 2 LSAs, and the summary net link states are type 3 LSAs.

The database columns are as follows:

- **Link ID:** Identifies each LSA.
- **ADV Router:** Advertising router; the source router of the LSA.
- **Age:** The maximum age counter in seconds; the maximum age is 1 hour or 3600 seconds.
- **Seq#:** Sequence number of the LSA; this number begins at 0x80000001 and increases with each update of the LSA.
- **Checksum:** Checksum of the individual LSA to ensure reliable receipt of that LSA.
- **Link count:** Total number of directly attached links used only on router LSAs. The link count includes all point-to-point, transit, and stub links. Each serial link counts as two, and each Ethernet link counts as one.

Interpreting the Routing Table: Types of Routes

Cisco.com

Route Designator		Description
O	OSPF interarea (router LSA)	<ul style="list-style-type: none">• Networks from within the area of the router• Advertised by way of router LSAs
O IA	OSPF inter-area (summary LSA)	<ul style="list-style-type: none">• Networks from outside the area of the router, but within the OSPF autonomous system• Advertised by way of summary LSAs
O E1	Type 1 external routes	<ul style="list-style-type: none">• Networks outside of the autonomous system of the router• Advertised by way of external LSAs
O E2	Type 2 external routes	

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-18

slide 21

The table defines each of the OSPF routing designators. Router and network LSAs describe the details within an area. The routing table reflects this link-state information with a designation of O, meaning the route is intra-area.

When an ABR or ASBR receives summary or external LSAs, it adds them to its LSDB and floods them to their local area. The internal routers then assimilate the information into their databases. Summary LSAs appear in the routing table as IA (interarea routes). External LSAs appear in the routing table marked as external type 1 (E1) or external type 2 (E2) routes.

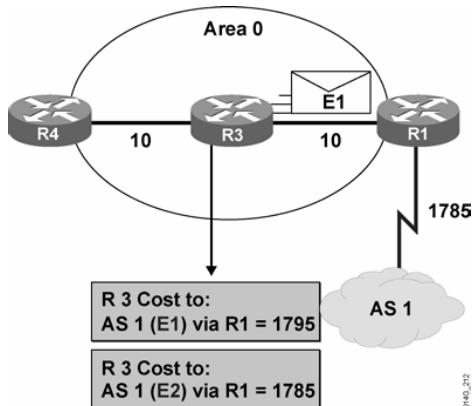
The SPF algorithm is then run against the LSDB to build the SPF tree. The SPF tree is used to determine the best paths. The order in which the best paths are calculated is as follows:

- Step 1** All routers calculate the best paths to destinations within their area (intra-area) and add these entries to the routing table. These are the type 1 and type 2 LSAs, which are noted in the routing table with a routing designator of O (OSPF).
- Step 2** All routers calculate the best paths to the other areas within the internetwork. These best paths are the interarea route entries, or type 3 and type 4 LSAs, and are noted with a routing designator of O IA (interarea).
- Step 3** All routers except those that are in the form of stub area calculate the best paths to the external autonomous system (type 5) destinations, and are noted with either an O E1 or an O E2 route designator, depending on configuration.

At this point, a router can communicate with any network within or outside the OSPF autonomous system.

Calculating Costs for External Type 1 and Type 2 Routes

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-19

The cost of an external route varies depending on the external type configured on the ASBR. The following external packet types can be configured:

- **E1:** Type O E1 external routes calculate the cost by adding the external cost to the internal cost of each link that the packet crosses. Use this type when there are multiple ASBRs advertising an external route to the same autonomous system to avoid suboptimal routing.
- **E2 (default):** The external cost of O E2 packet routes is always the external cost only. Use this type if only one ASBR is advertising an external route to the autonomous system.

The show ip route Command

Cisco.com

```
RTA# show ip route

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

Gateway of last resort is 203.250.15.67 to network 0.0.0.0
  203.250.16.0 255.255.255.192 is subnetted, 1 subnets
O E2  203.250.16.128 [110/10] via 203.250.15.67, 00:00:50, Ethernet0
  203.250.13.0 255.255.255.255 is subnetted, 1 subnets
C    203.250.13.41 is directly connected, Loopback0
  203.250.15.0 255.255.255.192 is subnetted, 3 subnets
O IA   203.250.15.0 [110/74] via 203.250.15.67, 00:00:50, Ethernet0
C    203.250.15.64 is directly connected, Ethernet0
C    203.250.15.192 is directly connected, Ethernet1
O*E2  0.0.0.0 0.0.0.0 [110/10] via 203.250.15.67, 00:00:50, Ethernet0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-21

The **show ip route** command example in this figure depicts both external type routes (O E2) and interarea (O IA) routes. The last entry (O *E2) is a default route from the ABR.

The two numbers in brackets, [110/10], are the administrative distance and the total cost of the route to a specific destination network. In this case, the administrative distance is set to a default of 110 for all OSPF routes, and the total cost of the route has been calculated as 10.

Changing the Cost Metric

Cisco.com

- Dijkstra's algorithm determines the best path by adding all link costs along a path.
- The cost, or metric, is an indication of the overhead to send packets over an interface.

RouterA(config-if)#

```
ip ospf cost value
```

- This interface configuration command overrides the default cost calculation. Values from 1 to 65535 can be defined.

RouterA(config-router)#

```
auto-cost reference-bandwidth
```

- This router ospf configuration command sets the reference bandwidth to values other than 100 Mbps (legal values range from 1 to 4,294,967).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-22

By default, OSPF calculates the OSPF metric for an interface according to the inverse bandwidth of the interface. In general, the cost in Cisco routers is calculated using the formula 100 Mbps per bandwidth.

For example, a 64-kbps link gets a metric of 1562, while a T1 link gets a metric of 64. However, the cost is calculated based on a maximum bandwidth of 100 Mbps, which is a cost of 1. If you have faster interfaces, you may want to recalibrate the cost of 1 to a higher bandwidth.

When you are using the bandwidth of the interface to determine OSPF cost, always remember to use the **bandwidth interface** command to accurately define the bandwidth per interface.

If interfaces that are faster than 100 Mbps are being used, you should consider the **auto-cost reference-bandwidth** command under the OSPF process. Use the **auto-cost reference-bandwidth** command on all routers in the network to ensure accurate route calculations.

To override the default cost, manually define the cost using the **ip ospf cost** command on a per-interface basis. The cost value is an integer from 1 to 65,535. The lower the number, the better and more strongly preferred the link.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- At this time, there are 11 different LSA types defined in OSPF. The first five are the most commonly used:
 - Type 1 router
 - Type 2 network
 - Type 3 and 4 summary
 - Type 5 external
- OSPF defines three kinds of routes: intra-area, interarea, and external. External routes are subdivided into E1 and E2.
- The cost metric default is the inverse of the bandwidth defined on an interface. The ospf cost command, the bandwidth command, and the auto-cost reference-bandwidth command can manipulate the cost metric.

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 benefits relate to a multiarea design in OSPF? (Choose three.)

- A) reduced LSA flooding
- B) reduced SPF calculations
- C) reduced size of the neighbor table
- D) reduced size of the database

Q2) Which router is not an OSPF router type?

- A) backbone
- B) ABR
- C) ASBR
- D) core

Q3) List the four different link types that a type 1 LSA defines.

- A) _____
- B) _____
- C) _____
- D) _____

Q4) Match each LSA name with the number corresponding to its LSA type.

- A) external
- B) network
- C) summary
- D) multicast
- E) router
- F) opaque
- G) NSSA

_____ 5

_____ 2

_____ 3 and 4

_____ 6

_____ 1

_____ 9 11

_____ 7

Q5) Which of the following items is NOT described in the **show ip ospf database** command?

- A) advertising router
- B) maximum age counter
- C) link counter
- D) LSA type
- E) link type

Q6) If the OSPF routing table shows an O E1 route, what does this mean?

- A) It is an interarea route that uses the external cost plus the interarea cost.
- B) It is an interarea route that uses the external cost only.
- C) It is an external route that uses the external cost only.
- D) It is an external route that uses the external cost plus the internal cost.

Quiz Answer Key

Q1) A, B, D

Relates to: Types of OSPF Routers

Q2) D

Relates to: Types of OSPF Routers

Q3) A-point-to-point

B-transit

C-stub

D-virtual link

Relates to: OSPF LSA Types

Q4) A-5, B-2, C-3 and 4, D-6, E-1, F-9 and 11, G-7

Relates to: OSPF LSA Types

Q5) E

Relates to: Interpreting the OSPF LSDB and Routing Table

Q6) D

Relates to: Interpreting the OSPF LSDB and Routing Table

OSPF Route Summarization Techniques

Overview

One of the key features of OSPF is the ability to summarize routes at area and autonomous system boundaries. Route summarization is important because it reduces OSPF LSA flooding and LSDB and routing table sizes, which reduces memory and CPU utilization on the routers. The OSPF network can scale to very large sizes in part because of route summarization. This lesson defines different types of route summarization and describes the configuration commands for each.

Relevance

Scalability, CPU and memory utilization, and the ability to mix small routers with large routers are all benefits of using proper route summarization techniques. Route summarization features are among the most important features of OSPF.

Objectives

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

- Describe route summarization
- Use route summarization commands for OSPF
- Use the **default-information originate** command to propagate a default route into OSPF
- Identify a default route in OSPF

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Knowledge of IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **OSPF Route Summarization Concepts**
- **OSPF Route Summarization Commands**
- **Creating a Default Route in OSPF**
- **The default-information originate command**
- **Summary**
- **Quiz**

OSPF Route Summarization Concepts

Route summarization is a key to scalability in OSPF. Route summarization helps solve two major problems: large routing tables and frequent LSA flooding throughout the autonomous system. This topic describes why it is important to always summarize OSPF routes.

Benefits of Route Summarization

Cisco.com

- Minimizes number of routing table entries
- Localizes impact of a topology change
- Reduces LSA type 3 and 5 flooding and saves CPU resources

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 4-4

Route summarization is the consolidation of multiple routes into a single advertisement. By this point, however, a network operator should realize the importance of proper route summarization in a network. Route summarization directly affects the amount of bandwidth, CPU, and memory resources consumed by the OSPF routing process.

Without route summarization, every specific-link LSA is propagated into the OSPF backbone and beyond, causing unnecessary network traffic and router overhead. Whenever an LSA is sent, all affected OSPF routers have to recompute their LSDB and the SPF tree using the SPF algorithm.

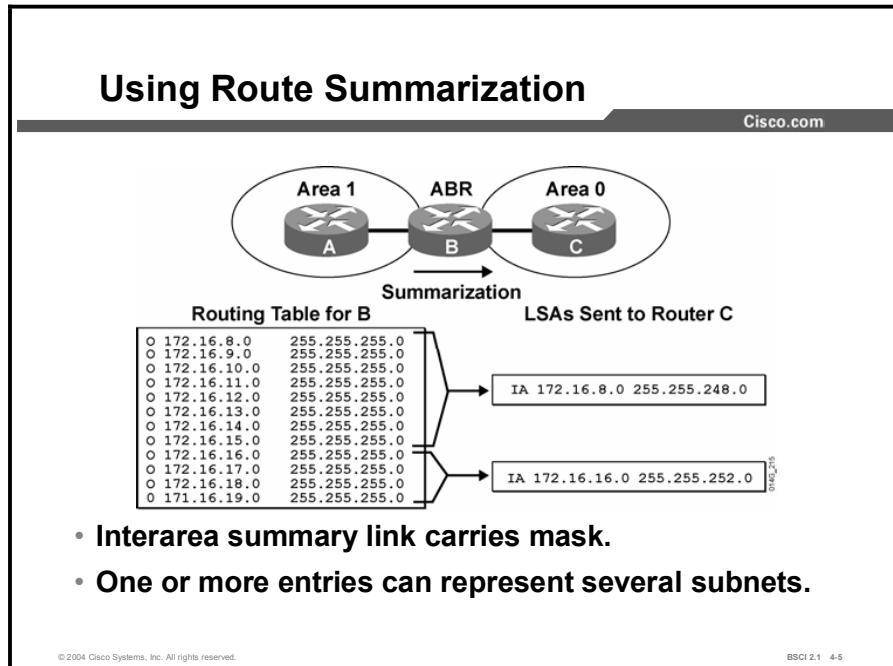
With route summarization, only summarized routes propagate into the backbone (area 0). This summarization is important because it prevents every router from having to rerun the SPF algorithm, increases the stability of the network, and reduces unnecessary LSA flooding. Also, if a network link fails, the topology change is not propagated into the backbone (and other areas by way of the backbone). LSA flooding outside the area does not occur.

Note	Summary LSAs (type 3 LSAs) do not always contain summarized routes. By default, summary LSAs are not summarized.
-------------	--

The two types of summarization are as follows:

- **Interarea route summarization:** Interarea route summarization occurs on ABRs and applies to routes from within each area. It does not apply to external routes injected into OSPF via redistribution. To perform effective interarea route summarization, network numbers within areas should be assigned contiguously so that these addresses can be summarized into a minimal number of summary addresses. The figure illustrates interarea summarization at the ABR.
- **External route summarization:** External route summarization is specific to external routes that are injected into OSPF via route redistribution. Again, it is important to ensure the contiguity of the external address ranges that are being summarized. Summarizing overlapping ranges from two different routers could cause packets to be sent to the wrong destination. Only ASBRs generally summarize external routes.

Example



OSPF carries subnet mask information and therefore supports multiple subnet masks for the same major network. Discontiguous subnets are also supported by OSPF, because subnet masks are part of the LSDB. However, other protocols (such as RIPv1 and IGRP) do not support variable-length subnet masking (VLSM) or discontiguous subnets.

If the same major network crosses the boundaries of an OSPF and an RIPv1 or IGRP domain, then VLSM information redistributed into RIPv1 or IGRP is lost, and static routes have to be configured in the RIPv1 or IGRP domains.

Network numbers in areas should be assigned contiguously to ensure that these addresses can be summarized into a minimal number of summary addresses.

For example, in the figure, the list of 12 networks in the routing table of router B can be summarized into two summary address advertisements. The block of addresses from 172.16.8.0 through 172.16.15.0/24 can be summarized using 172.16.8.0/21, and the block from 172.16.16.0 through 172.16.19.0/24 can be summarized using 172.16.16.0/22.

OSPF Route Summarization Commands

This topic defines the specific configuration commands required for interarea and external route summarization in OSPF.

Configuring Route Summarization

Cisco.com

```
Router(config-router)#
area area-id range address mask
```

- **Consolidates interarea routes on an ABR**

```
Router(config-router)#
summary-address address mask [not-advertise] [tag tag]
```

- **Consolidates external routes, usually on an ASBR**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 4-6

OSPF is a classless routing protocol; therefore, it does not perform autosummarization. Manual summarization for OSPF is off by default. To configure manual interarea route summarization on the ABR, use the following procedure:

- Step 1** Configure OSPF.
- Step 2** Use the **area range** command to instruct the ABR to summarize routes for a specific area before injecting them into a different area via the backbone as type 3 summary LSAs.

The table describes the parameters for the **area range** command.

area range Parameters

Parameter	Description
area-id	Identifies the area subject to route summarization
address	Summary address designated for a range of addresses
mask	IP subnet mask used for the summary route

To configure manual route summarization on an ASBR to summarize external routes, complete the following steps:

- Step 1** Configure OSPF.

- Step 2** Use the **summary-address** command to instruct the ASBR or the ABR to summarize external routes before injecting them into the OSPF domain as type 5 external LSA.

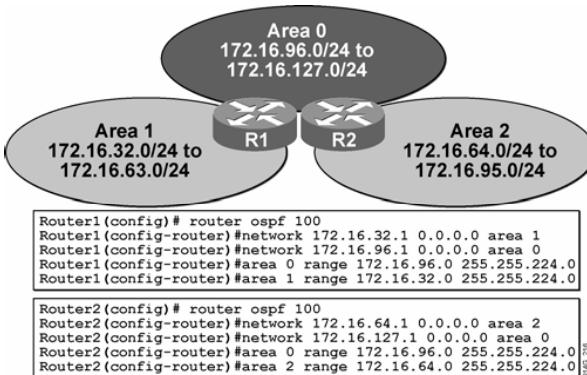
The table describes the parameters of the **summary-address** command.

summary-address Parameters

Parameter	Description
address	Summary address designated for a range of addresses
mask	IP subnet mask used for the summary route
not-advertise	(Optional) Used to suppress routes that match the prefix and mask pair
tag tag	(Optional) Tag value that can be used as a match value for controlling redistribution via route maps

Route Summarization Configuration Example at ABR

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

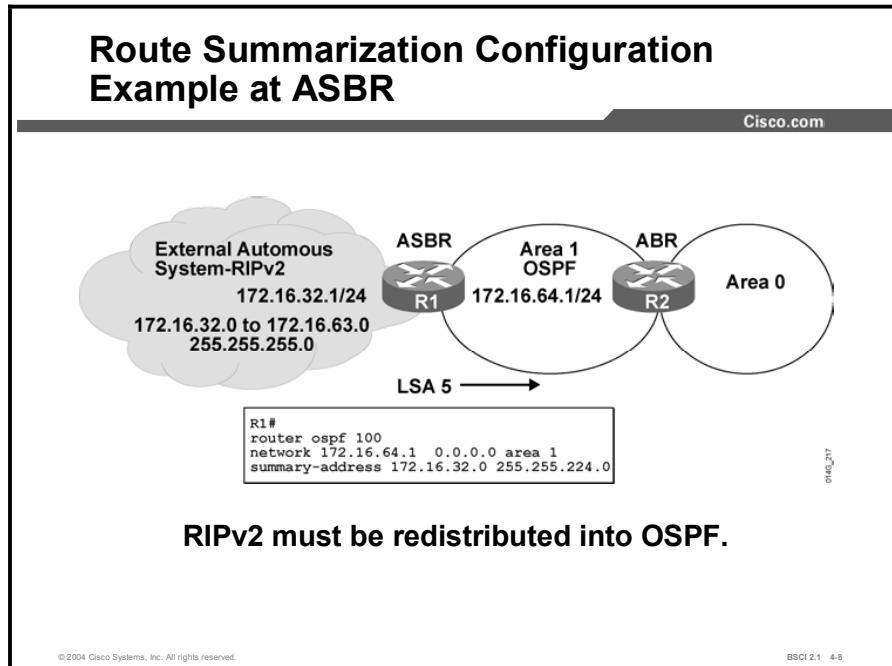
The figure shows that route summarization can occur in both directions: from a nonbackbone area to area 0, and from area 0 to a nonbackbone area. In the example, the router 1 configuration specifies the following summarization:

- **area 0 range 172.16.96.0 255.255.224.0:** Identifies area 0 as the area containing the range of networks to be summarized into area 1. ABR router 1 summarizes the range of subnets from 172.16.96.0 to 172.16.127.0 into one range: 172.16.96.0 255.255.224.0.
- **area 1 range 172.16.32.0 255.255.224.0:** Identifies area 1 as the area containing the range of networks to be summarized into area 0. ABR router 1 summarizes the range of subnets from 172.16.32.0 to 172.16.63.0 into one range: 172.16.32.0 255.255.224.0.

The configuration for router 2 works similarly.

Note	Depending on your network topology, you may not want to summarize area 0 networks. For example, if you have more than one ABR between an area and the backbone area, sending a summary LSA with the explicit network information ensures that the shortest path is selected. If you summarize the addresses, suboptimal path selection may occur.
-------------	---

Example



The figure depicts route summarization at the ASBR. On the left, an external autonomous system running Routing Information Protocol version 2 (RIPv2) has its routes redistributed into OSPF.

Because of the contiguous subnet block in the external RIP network, it is possible to summarize the 32 different subnets into one summarized route. Instead of 32 external type 5 LSAs flooding into the OSPF network, there is only one.

Creating a Default Route in OSPF

Occasionally, you will be required to configure OSPF to advertise a default route into its autonomous system. This topic defines the use of a default route and how it is configured under OSPF.

Default Routes in OSPF

Cisco.com

The diagram illustrates the OSPF network configuration. On the left, an oval labeled 'OSPF Autonomous System' contains the IP address '10.1.1.1'. A router labeled 'R1' with the IP '198.1.1.1' is connected to R1. Router R1 is also connected to another router with the IP '198.1.1.2', which is connected to a cloud labeled 'Internet Service Provider'. An arrow points from the '0.0.0.0' default route to the '198.1.1.2' interface of R1.

- A default route is injected into OSPF as an external LSA type 5.
- Default route distribution is not on by default; use a default-information originate command under the OSPF routing process.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

The figure shows how OSPF injects a default route into a normal area. Any OSPF router can originate default routes injected into a normal area. The OSPF router does not, by default, generate a default route into the OSPF domain. In order for OSPF to generate a default route, you must use the **default-information originate** command.

There are two ways to advertise a default route into a normal area. The first is to advertise 0.0.0.0 into the OSPF domain, provided that the advertising router already has a default route. The second is to advertise 0.0.0.0 regardless of whether the advertising router already has a default route. The second method can be accomplished by adding the keyword **always** to the **default-information originate** command.

A default route shows up in the OSPF database as an external LSA type 5. Here is an example of how it looks in the database:

Type-5 AS External Link States					
Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	198.1.1.1	601	0x80000001	0xD0D8	0

The default-information originate Command

This topic defines the mechanics of configuring a default route injection into OSPF.

Configuring OSPF Default Routes

Cisco.com

```
Router(config-router)#  
      default-information originate [always]
```

- A router ospf subordinate command.
- Normally, this command only advertises a 0.0.0.0 default into the OSPF network if the default route already exists in the routing table.
- The always keyword allows the 0.0.0.0 default to be advertised even when the default route does not exist in the routing table.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-10

To generate a default external route into an OSPF routing domain, use the **default-information originate** router configuration command:

```
[no] default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

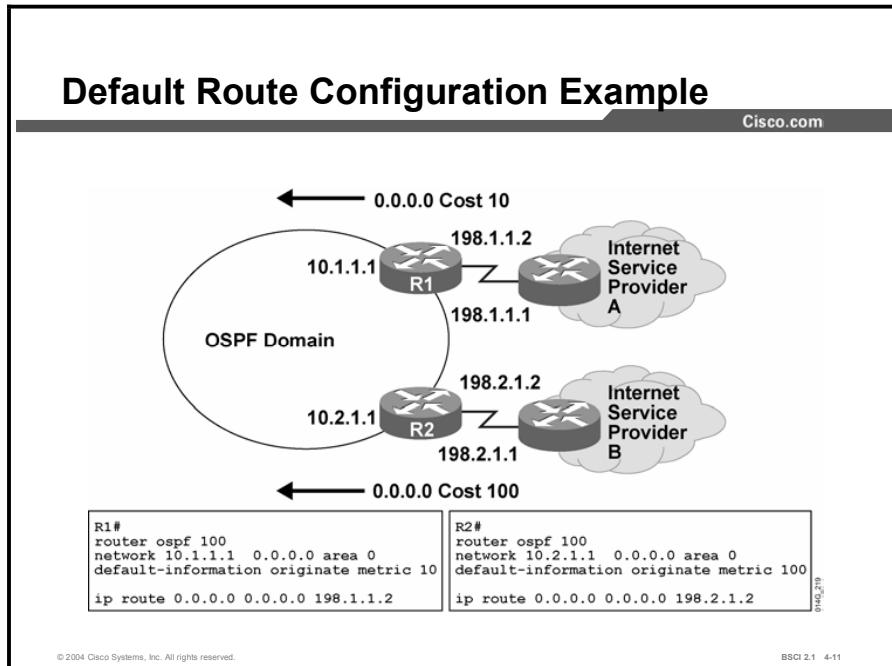
To disable this feature, use the **no** form of this command.

The table describes the parameters of the command.

default-information originate Parameters

Parameter	Description
always	(Optional) Always advertises the default route regardless of whether the software has a default route in the routing table.
metric metric-value	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 10. The value used is specific to the protocol.
metric-type type-value	(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: 1: type 1 external route 2: type 2 external route The default is type 2 external route (O *E2).
route-map map-name	(Optional) Routing process generates the default route if the route map is satisfied.

Example



In the figure, an OSPF network is multihomed to dual Internet service providers (ISPs). Provider A is preferred, and provider B is used as a backup. The optional **metric** command has been used to establish a preference for the default route to ISP A.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Route summarization improves CPU utilization, reduces LSA flooding, and reduces LSDB and routing table sizes.**
- **The area range command is used to summarize at the ABR.**
- **The summary-address command is used to summarize at the ASBR.**
- **Default routes can be used in OSPF to prevent the need for a specific route to all destination networks. The benefit is a much smaller routing table and LSDB, with complete reachability.**
- **OSPF uses a special command to inject a default route, called the default-information originate command.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

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 reasons why route summarization is important? (Choose two.)
- A) reduces LSA type 1 flooding
 - B) reduces LSA type 3 flooding
 - C) reduces the size of the routing table
 - D) reduces the size of the neighbor table
- Q2) Which two features play a key role in route summarization? (Choose two.)
- A) network numbers in areas should be assigned contiguously
 - B) network numbers in areas should be assigned discontiguously
 - C) FLSM
 - D) VLSM
- Q3) Which command would you use to summarize routes into area 0 from the ABR?
- A) **summary-address**
 - B) **area x range**
 - C) **network**
 - D) **area x summary**
- Q4) Which command would you use to summarize routes into OSPF from the ASBR?
- A) **summary-address**
 - B) **area x range**
 - C) **network**
 - D) **area x summary**
- Q5) A default route is identified in the OSPF database as an _____.
- A) LSA type 1
 - B) LSA type 2
 - C) LSA type 3
 - D) LSA type 4
 - E) LSA type 5
- Q6) The primary purpose of a default route is to reduce the routing table and LSDB size. A default route avoids detailed updating of routes by inserting a single 0.0.0.0 into the routing table, making this 0.0.0.0 route act as a gateway of last resort.
- A) true
 - B) false

- Q7) When should you use the **always** keyword with the **default-information originate** command?
- A) on by default; configuration not required
 - B) when you want to send summarized routes
 - C) when your default route is always in the routing table
 - D) when you want the default route advertised, even if it is not in the routing table
- Q8) Default routes must always be O E2 routes; there is no other choice.
- A) true
 - B) false

Quiz Answer Key

Q1) B, C

Relates to: OSPF Route Summarization Concepts

Q2) A, D

Relates to: OSPF Route Summarization Concepts

Q3) B

Relates to: OSPF Route Summarization Commands

Q4) A

Relates to: OSPF Route Summarization Commands

Q5) E

Relates to: Creating a Default Route In OSPF

Q6) A

Relates to: Creating a Default Route In OSPF

Q7) D

Relates to: The default-information originate Command

Q8) B

Relates to: The default-information originate Command

OSPF Special Area Types

Overview

OSPF defines several special-case area types used by the network operator. These special cases include stub areas, totally stubby areas, and not-so-stubby areas (NSSAs). The general purpose behind all three types of stub areas is to inject default routes into an area so that external or summary LSAs are not flooded in. Stub areas are designed to reduce the amount of flooding, the LSDB size, and the routing table size in routers within the area.

Relevance

Network designers should always consider using stub area techniques when building networks. Stub area techniques improve performance in OSPF networks and allow the network to scale to significantly large sizes.

Objectives

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

- List the types of OSPF areas
- Define and configure OSPF stub areas
- Define and configure OSPF totally stubby areas
- Define and configure OSPF NSSAs

Learner Skills and Knowledge

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

- General knowledge of distance vector protocols
- Knowledge of IP subnetting
- General knowledge of the Cisco IOS software user interface
- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

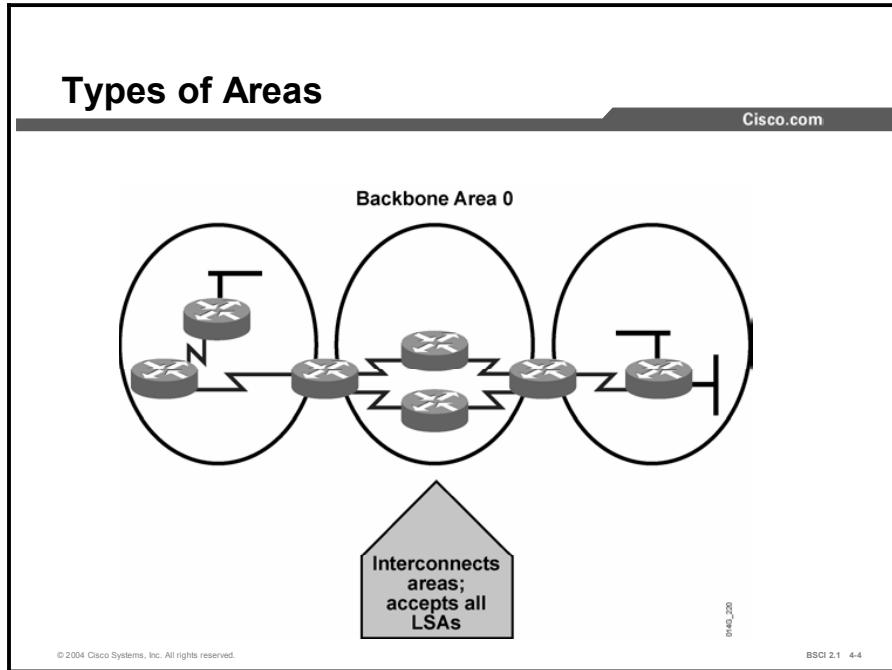
Outline

Cisco.com

- **Overview**
- **Types of OSPF Areas**
- **Stub Areas**
- **Totally Stubby Areas**
- **Not-So-Stubby Areas**
- **Summary**
- **Quiz**

Types of OSPF Areas

This topic briefly identifies the various kinds of OSPF areas that are configurable.



The characteristics assigned to an area control the type of route information that it receives. The possible area types are as follows:

- **Standard area:** This default area accepts link updates, route summaries, and external routes.
 - **Backbone area (transit area):** The backbone area is the central entity to which all other areas connect. The backbone area is labeled area 0. All other areas connect to this area to exchange and route information. The OSPF backbone has all the properties of a standard OSPF area.
 - **Stub area:** This area does not accept information about routes external to the autonomous system, such as routes from non-OSPF sources. If routers need to route to networks outside the autonomous system, they use a default route, noted as 0.0.0.0. Stub areas cannot contain ASBRs.
 - **Totally stubby area:** This area does not accept external autonomous system routes or summary routes from other areas internal to the autonomous system. If the router needs to send a packet to a network external to the area, it sends the packet using a default route. Totally stubby areas cannot contain ASBRs.
 - **NSSA:** NSSA is an addendum to the OSPF RFC. This area defines a special LSA type 7. An NSSA offers benefits that are similar to those of a stub or totally stubby area. However, NSSAs allow ASBRs, which is against the rule in a stub area.

Stub Area Rules

Cisco.com

- **Stub areas cannot have an ASBR, and they should have one ABR.**
- **If there is more than one ABR, suboptimal routing paths to external autonomous systems can occur.**
- **Stub areas must not have virtual links going through them.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

Stub and totally stubby areas do not carry any external routes, known as type 5 LSAs. An area can be qualified as a stub or totally stubby if it has the following characteristics:

- There is a single exit point from that area, or there are multiple exits, such as ABRs routing to the outside of the area that do not have to take an optimal path. If the area has multiple exits, one or more ABRs inject a default into the stub area. In this situation, routing to other areas or autonomous systems could take a suboptimal path to reach the destination by exiting the area via a point that is farther from the destination than other exit points.
- All OSPF routers inside the stub area, including ABRs and internal routers, must be configured as stub routers before they can become neighbors and exchange routing information.
- The area is not needed as a transit area for virtual links.
- No ASBR is inside the stub area.
- The area is not the backbone area, area 0.

Stub Areas

This topic describes stub areas and how to configure them.

Using Stub Areas

Cisco.com

- External LSAs are stopped.
- Default route is advertised into stub area by the ABR.
- All routers in area 50 must be configured as stub.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-8

Configuring a stub area reduces the size of the LSDB inside an area, resulting in reduced memory requirements for routers in that area. External network LSAs (type 5), such as those redistributed from other routing protocols into OSPF, are not permitted to flood into a stub area.

Routing from these areas to the outside is based on a default route (0.0.0.0). In the case of a default route, if a packet is addressed to a network that is not in the route table of an internal router, the router automatically forwards the packet to the ABR that sends a 0.0.0.0 LSA. Forwarding the packet to the ABR allows routers within the stub to reduce the size of their routing tables because a single default route replaces many external routes.

A stub area is typically created using a hub-and-spoke topology, with the spoke being the stub area, such as a branch office. In this case, the branch office does not need to know about every network at the headquarters site because it can use a default route to reach the networks.

Stub Area Configuration

Cisco.com

```
RouterA(config-router)#
```

```
Area area-id stub
```

- **This router subordinate command turns on stub area networking.**
- **All routers in a stub area must use the stub command.**

```
router ospf 10
  network 130.130.32.0 0.0.31.255 area 1
  network 130.130.0.0 0.0.31.255 area 0
  area 1 stub
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

To configure an area as a stub, complete the following steps:

Step 1 Configure OSPF.

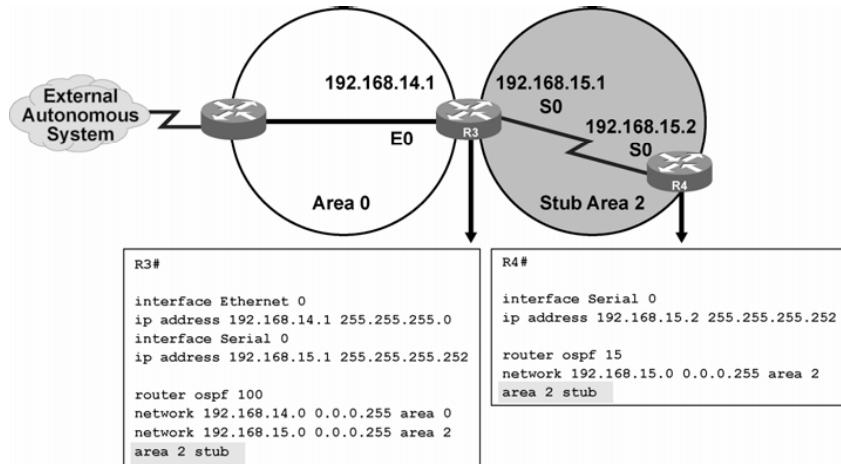
Step 2 Define an area as stub or totally stubby by issuing the **area area-id stub** command to all routers within the area. The table lists the parameters of this command.

area stub Parameters

Parameter	Description
<i>area-id</i>	Identifier for the stub or totally stubby area. The identifier can be either a decimal value or a value in dotted-decimal format like an IP address.

OSPF Stub Area Configuration Example

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 4-10

Area 2 in the figure is defined as the stub area. No routes from the external autonomous system are forwarded into the stub area.

The last line in each configuration (**area 2 stub**) defines the stub area. Router 3 (ABR) automatically advertises 0.0.0.0 (the default route) with a default cost metric of 1 into the stub area.

Each router in the stub area must be configured with the **area stub** command.

The routes that appear in the routing table of router 4 are as follows:

- Intra-area routes, which are designated with an O in the routing table
- The default route and interarea routes, which are both designated with an IA in the routing table
- The default route, which is also denoted with an asterisk (O *IA)

Note

The **area area-id stub** command determines whether the routers in the stub become neighbors. This command is enabled on all routers in the stub to permit the exchange of routing information. The hello packet contains a stub area flag that must match on neighboring routers.

Totally Stubby Areas

The totally stubby area technique is an enhancement to a stub area. This topic describes totally stubby areas and how they are configured.

Using Totally Stubby Areas

Cisco.com

- External LSAs are stopped.
- Summary LSAs are stopped.
- Routing table is reduced to a minimum.
- All routers must be configured as stub.
- ABR must be configured as totally stubby.
- This is a Cisco proprietary feature.

The diagram illustrates an OSPF network topology. Area 50 (Totally Stub) contains two routers. Area 0 (Area Border Router) contains three routers: ABR1, ASBR, and ABR2. Area 51 (Regular) contains one router. ABR1 connects Area 50 and Area 0. ABR2 connects Area 0 and Area 51. ASBR connects Area 0 to an RIP network. LSAs shown: Internal, Summary, Default, and External.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-11

A totally stubby area is a Cisco proprietary feature that further reduces the number of routes in the routing table. A totally stubby area is a stub area that blocks external type 5 LSAs and summary type 3 and type 4 LSAs (interarea routes) from entering the area.

By blocking these routes, the totally stubby area recognizes only intra-area routes and the default route of 0.0.0.0. ABRs inject the default summary link 0.0.0.0 into the totally stubby area. Each router picks the closest ABR as a gateway to everything outside the area.

Totally stubby areas minimize routing information further than stub areas and increase stability and scalability of OSPF internetworks. Using totally stubby areas is typically a better solution than using stub areas as long as the ABR is a Cisco router.

Totally Stubby Commands

Cisco.com

RouterA(config-router)#

```
area area-id stub no-summary
```

- The addition of **no-summary** creates a totally stubby area.
- The **no-summary** option prevents all summary LSAs from entering the stub area.

RouterA(config-router)#

```
area area-id default-cost cost
```

- This command defines the cost of a default route sent into the stub area.
- The default cost is 1.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-12

To configure an area as totally stubby, complete the following steps:

Step 1 Configure OSPF.

Step 2 Define an area as stub or totally stubby by issuing the **area area-id stub** command to all routers within the area.

Step 3 At the ABR only, add **no-summary** to the **area area-id stub** command.

The ABR will advertise a default route with a cost of 1. An option is to change the cost of the default route by using the **area area-id default-cost** command.

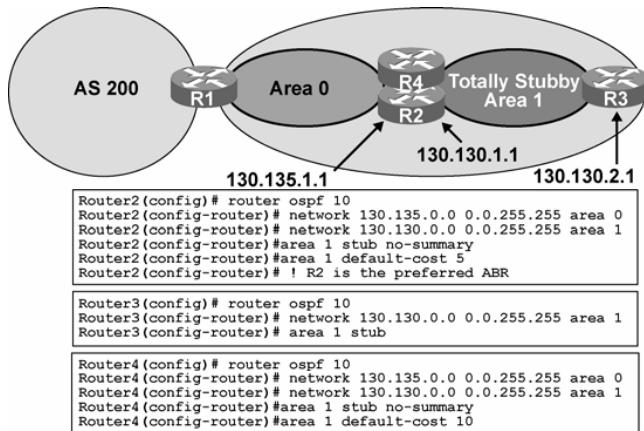
The table describes the parameters of the **area stub** command.

area stub Parameters

Parameter	Description
<i>area-id</i>	Identifier for the stub or totally stubby area. The identifier can be either a decimal value or a value in dotted-decimal format like an IP address.
no-summary	In addition to stopping external LSA flooding, the no-summary command also prevents summary LSAs from flooding into the totally stubby area.

Totally Stubby Configuration Example

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-13

9195220

The figure shows an example of a totally stubby area configuration. All routes advertised into area 1 (from area 0 and the external autonomous system) default to 0.0.0.0. The default route cost is set to 5 on router 2 and to 10 on router 4.

Both default routes are advertised into area 1. However, the default route from router 2 is advertised with a lower cost to make it preferable if the internal cost from router 3 to router 4 and router 2 is the same.

Notice that router 3 requires the **area 1 stub** command, yet the **no-summary** extension is not required. Only ABRs use **no-summary** to keep summary LSAs from being propagated into another area.

Note Remember that all routers in a stub or totally stubby area must be configured as stub. An OSPF adjacency will not form between stub and nonstub routers.

Routing Tables with Different Areas

Cisco.com

IP routing table for an OSPF regular area

```
plr3#show ip route
<Output Omitted>

10.0.0.0/24 is subnetted, 15 subnets
O IA 10.3.1.0 [110/148] via 10.64.0.2, 00:03:12, Ethernet0
C 10.1.3.0 is directly connected, Serial0
O IA 10.2.1.0 [110/74] via 10.64.0.2, 00:31:46, Ethernet0
C 10.1.2.0 is directly connected, Serial1
O IA 10.3.2.0 [110/149] via 10.64.0.2, 00:03:12, Ethernet0
O IA 10.2.2.0 [110/138] via 10.64.0.2, 00:31:46, Ethernet0
O IA 10.1.1.0 [110/128] via 10.1.3.1, 00:31:46, Serial0
[110/128] via 10.1.2.1, 00:31:46, Serial1
O IA 10.3.2.0 [110/212] via 10.64.0.2, 00:03:12, Ethernet0
O IA 10.2.3.0 [110/74] via 10.64.0.2, 00:31:46, Ethernet0
O IA 10.4.2.0 [110/286] via 10.64.0.2, 00:02:50, Ethernet0
O IA 10.4.3.0 [110/222] via 10.64.0.2, 00:02:50, Ethernet0
O IA 10.4.1.0 [110/222] via 10.64.0.2, 00:02:50, Ethernet0
O E2 10.66.0.0 [110/60] via 10.64.0.2, 00:02:51, Ethernet0
C 10.64.0.0 is directly connected, Ethernet0
O E2 10.65.0.0 [110/60] via 10.64.0.2, 00:03:19, Ethernet0
plr3#
```

All routes (interarea, intra-area, external)

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-14

This figure shows how the routing table of an OSPF router without stub or totally stubby configuration might look. Intra-area, interarea, and external routes are all maintained in a normal area without stub configuration.

Routing Tables for Stub Area

Cisco.com

```
plr3#show ip route
<Output Omitted>

Gateway of last resort is 10.64.0.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA 10.2.0.0/16 [110/74] via 10.64.0.2, 00:11:11, Ethernet0
C 10.1.3.0/24 is directly connected, Serial0
O IA 10.3.0.0/16 [110/148] via 10.64.0.2, 00:07:59, Ethernet0
C 10.1.2.0/24 is directly connected, Serial1
O 10.1.1.0/24 [110/128] via 10.1.3.1, 00:16:51, Serial0
[110/128] via 10.1.2.1, 00:16:51, Serial1
O IA 10.4.0.0/16 [110/222] via 10.64.0.2, 00:09:13, Ethernet0
C 10.64.0.0/24 is directly connected, Ethernet0
O*IA 0.0.0.0/0 [110/11] via 10.64.0.2, 00:16:51, Ethernet0
plr3#
```

IP routing table with route summarization and stub capabilities enabled

Route summaries that use route summarization

Default route to get to external autonomous systems

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-15

Routing Tables for Totally Stubby Area

Cisco.com

```
p1r3#show ip route
<Output Omitted>

Gateway of last resort is 10.64.0.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C      10.1.3.0/24 is directly connected, Serial0
C      10.1.2.0/24 is directly connected, Serial1
O      10.1.1.0/24 [110/128] via 10.1.3.1, 00:16:51, Serial0
          [110/128] via 10.1.2.1, 00:16:51, Serial1
C      10.64.0.0/24 is directly connected, Ethernet0
O*IA 0.0.0.0/0 [110/11] via 10.64.0.2, 00:16:51, Ethernet0
p1r3#
```

IP routing table with route summarization and stub capabilities enabled

Default route to get to external networks



©2004 Cisco Systems, Inc. All rights reserved.

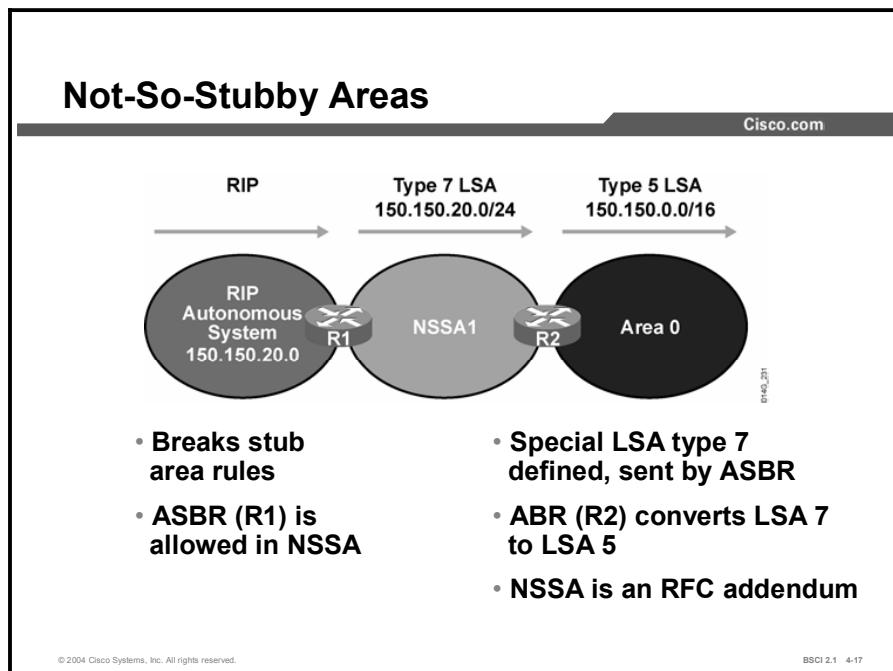
BSCI 2.1 4-16

The tables in the figures compare routing tables that result from the use of route summarization, stub areas, and totally stubby areas.

Note the interarea 0.0.0.0 default routes that appear in the stub and totally stubby area routers. Also, note that the totally stubby routers have the smallest routing table. All interarea summary routes, as well as all external routes, have been removed.

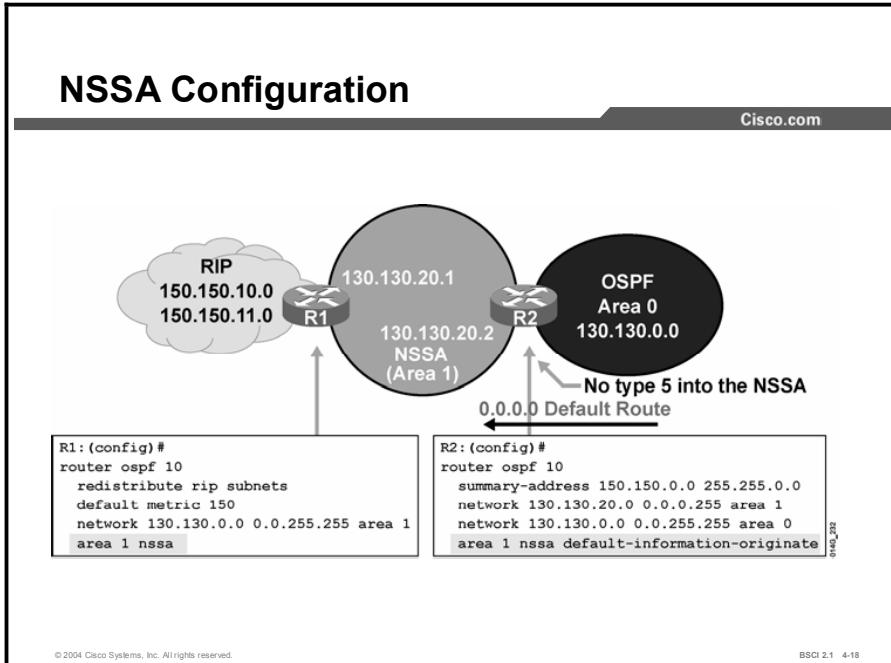
Not-So-Stubby Areas

The NSSA technique is described in this topic.



The OSPF NSSA feature is described by RFC 1587 and was first introduced in Cisco IOS Software Release 11.2. It is a nonproprietary extension of the existing stub area feature that allows the injection of external routes in a limited fashion into the stub area.

Redistribution into an NSSA creates a special type of LSA known as type 7, which can exist only in an NSSA. An NSSA ASBR generates this LSA, and an NSSA ABR translates it into a type 5 LSA, which gets propagated into the OSPF domain.



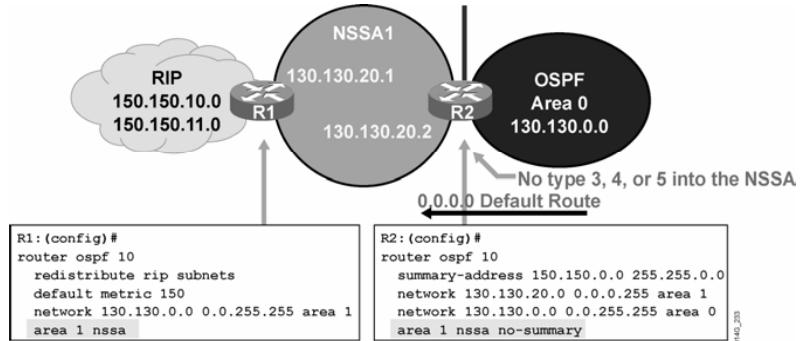
The **area area-id nssa** command is used in place of the **area area-id stub** command. Remember that all routers in the NSSA must have this command configured. Routers will not form an adjacency unless both are configured as NSSA.

In the figure, router 1 is the ASBR that is redistributing RIP routes into area 1, the NSSA. Router 2 is the NSSA ABR. This router converts LSA type 7 into type 5 for advertisement into the backbone area 0. Router 2 is also configured to summarize the type 5 LSAs that originate from the RIP network. The 150.150.0.0 subnets will be summarized to 150.150.0.0/16 and advertised into area 0.

To cause Router 2 (the NSSA ABR) to generate an O*N2 default route (O*N2 0.0.0.0/0) into the NSSA, use the **default-information-originate** option with the **area area-id stub** command at router 2.

NSSA Totally Stubby Configuration

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 4-19

Notice in the figure that the ABR is using the **area 1 nssa no-summary** command. This command works exactly the same as the totally stubby technique. A single default route replaces both inbound-external (type 5) LSAs and summary (type 3 and 4) LSAs into the area. The NSSA ABR, which is router 2, automatically generates the O*N2 default route into the NSSA area with the **no-summary** option configured at the ABR.

All other routers in the NSSA area require the **area 1 nssa** command only. The NSSA totally stubby configuration is a Cisco proprietary feature like the totally stubby area feature.

The show Commands for Stub and NSSA

Cisco.com

RouterA#

```
show ip ospf
```

- Displays which areas are normal, stub, or NSSA

RouterA#

```
show ip ospf database
```

- Displays LSA type 7 updates

RouterA#

```
show ip ospf database nssa-external
```

- Displays specific details of each LSA type 7 update in database

RouterA#

```
show ip route
```

- Displays NSSA routes with code O N2 or O N1

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-28

The **show** commands in the figure are used to display which area type has been configured. NSSA is different from the other area types because the router LSDB includes type 7 LSAs. The type 7 LSA is described in the routing table as an O N2 or O N1 (N means NSSA).

N1 means that the metric is calculated like external type 1; N2 means that the metric is calculated like external type 2. The default is O N2.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Several area types are defined in OSPF.**
- **The backbone is the transit area.**
- **Stub areas reduce flooding into the area by replacing external LSAs with a default route.**
- **Totally stubby areas reduce flooding into the area by replacing both external and summary LSAs with a default route.**
- **NSSAs are a special case. They allow an area that does not meet the requirements of a stub to gain the benefits of a stub.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-21

Next Steps

For the associated lab exercises, refer to the following sections of the course Lab Guide:

- Lab Exercise 4-2: Configuring OSPF for Multiple Areas and Frame Relay NBMA
- Lab Exercise 4-3: Configuring OSPF for Multiple Areas and Frame Relay Point-to-Multipoint and Point-to-Point
- Lab Exercise 4-4: Understanding the OSPF Database and Tuning 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 is NOT permitted in a stub area?
- A) an ABR
 - B) an ASBR
 - C) summary routes
 - D) summary LSAs
- Q2) Which type of router advertises the default into a stub area?
- A) ASBR
 - B) backbone router
 - C) ABR
 - D) internal router
- Q3) What is the correct configuration for stub area 10?
- A) **area 10 stub-area**
 - B) **router ospf 10 stub**
 - C) **area 10 stub**
 - D) **area 10 stub no-summary**
- Q4) What does the **no-summary** command mean?
- A) There is no route summarization in the stub area.
 - B) No summary LSAs are allowed into the stub area.
 - C) There is no LSA type 5 in the stub area.
 - D) There are no external LSAs in the stub area.
- Q5) The default route has a cost of 1 applied to it from the ABR if no area **default-cost** command is used.
- A) true
 - B) false
- Q6) Which characteristic relates to NSSA?
- A) allows stub area benefits without meeting stub area requirements
 - B) is a Cisco proprietary technique
 - C) allows ASBRs but not virtual links
 - D) floods LSA type 7 into the backbone area

Q7) A disadvantage of NSSA is that it does not have a totally stubby feature like a normal stub area.

- A) true
- B) false

Quiz Answer Key

Q1) B

Relates to: Types of OSPF Areas

Q2) C

Relates to: Stub Areas

Q3) C

Relates to: Stub Areas

Q4) B

Relates to: Totally Stubby Areas

Q5) A

Relates to: Totally Stubby Areas

Q6) A

Relates to: Not-So-Stubby Areas

Q7) B

Relates to: Not-So-Stubby Areas

OSPF Virtual Links

Overview

You should use the virtual link feature in OSPF in very specific cases. Virtual links are generally used for temporary connections or backup after a failure. A virtual link is a link that allows an area to connect to the backbone via a transit area. The transit area cannot be a stub area. This lesson defines when you should consider virtual links and how to configure them.

Relevance

Virtual links are important for the following:

- Temporary area connectivity, such as moves, adds, or changes
- Backup in the event of failure

Virtual links should not be used as a primary backbone design feature.

Objectives

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

- Define the two major purposes of OSPF virtual links
- Configure OSPF virtual links
- Verify OSPF virtual links operation

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Defining an OSPF Virtual Link**
- **Configuring OSPF Virtual Links**
- **Verifying OSPF Virtual Links Operation**
- **Summary**
- **Quiz**

Defining an OSPF Virtual Link

This topic defines the two major purposes of OSPF virtual links.

Illegal Area Connections

- By default, all areas must connect to area 0.
- Area 4 is connected incorrectly.
- There may be times when this type of connectivity is required.

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 4-4
0140_294

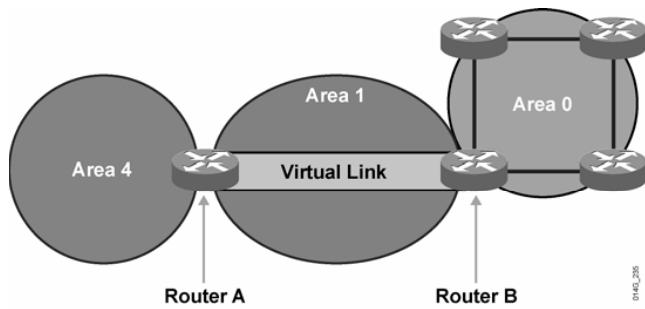
The two-tiered area hierarchy of OSPF requires that all areas directly connect to the backbone area, area 0. In the figure, area 4 is incorrectly connected to area 1. This incorrect connection leads to LSDB inconsistencies and reachability issues between area 4 networks and area 0.

Two major reasons why a virtual link is necessary are the following:

- **Backup:** Area 4 is normally directly attached to area 0; however, in the figure, the physical link between area 4 and area 0 is broken. Configure a backup link using area 1 as a transit area to reconnect area 4 temporarily to area 0. The transit area cannot be a stub area. Backup may also be required when area 0 separates into disconnected pieces because of a failed link.
- **Temporary connection:** Due to moves, adds, or changes, area 4 may be a new company acquisition that requires temporary connectivity. A virtual link could be used temporarily, until a more correct configuration, connecting area 4 directly to area 0, can be implemented.

Defining Virtual Links

Cisco.com



- **Virtual links are used to connect a discontiguous area to area 0.**
- **A logical connection is built between router A and router B.**
- **Virtual links are recommended for backup or temporary connections.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-5

Virtual links are part of the OSPF open standard and have been a part of Cisco IOS software since Software Release 10.0. In the figure, a logical link (virtual link) is built between the two ABRs, routers A and B. This virtual link is similar to a standard OSPF adjacency; however, in a virtual link, the routers do not have to be directly attached to neighboring routers.

The Hello protocol works over virtual and standard links in the same way: in 10-second intervals. The LSA updates work uniquely on virtual links. An LSA usually refreshes every 30 minutes; however, LSAs learned through the virtual link have the DoNotAge (DNA) option set. If the DNA option is set in the LSA, the LSA does not age out. The DNA technique is required to prevent excessive flooding over the virtual link.

Configuring OSPF Virtual Links

This topic describes the virtual link configuration process. This topic also discusses using the **show ip ospf virtual-link** command to ensure the virtual link works properly.

Configuring Virtual Links

Cisco.com

```
Router(config-router)#  
area area-id virtual-link router-id
```

- Creates a virtual link

```
remotercuter# show ip ospf interface ethernet 0  
  
Ethernet0 is up, line protocol is up  
  Internet Address 10.64.0.2/24, Area 0  
  Process ID 1, Router ID 10.64.0.2, Network Type BROADCAST, Cost: 10  
  Transmit Delay is 1 sec, State DR, Priority 1  
  Designated Router (ID) 10.64.0.2, Interface address 10.64.0.2  
  Backup Designated router (ID) 10.64.0.1, Interface address 10.64.0.1
```

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 4-6

Use the **area area-id virtual-link link router-id** router configuration command, along with any necessary optional parameters, to define an OSPF virtual link. To remove a virtual link, use the **no** form of this command.

```
area area-id virtual-link router-id [authentication [message-digest | null]] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [[authentication-key key] | [message-digest-key key-id md5 key]]
```

The **virtual-link** command requires a configured router ID from the far-end router. To find the router ID in the far-end router, use the **show ip ospf** command. An alternative is using the **show ip protocol** command. Both these commands display the router ID.

The following table describes the options available with the **virtual-link** command. Make sure that you understand the effect of these options before changing them. For instance, the smaller the hello interval, the faster the detection of topological changes; however, more routing traffic ensues.

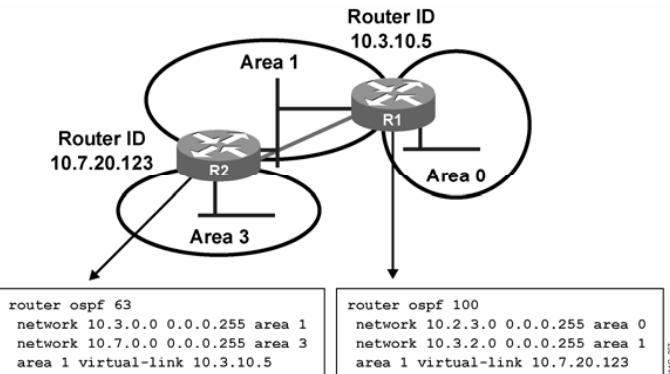
You should be conservative with the setting of the retransmit interval, or the result is needless retransmissions. The value is larger for serial lines and virtual links. The transmit delay value should take into account the transmission and propagation delays for the interface. Cisco IOS software uses the specified authentication key only when authentication is enabled with the **area area-id authentication** router configuration command. The two authentication schemes (simple text and Message Digest 5 [MD5] authentication) are mutually exclusive.

virtual-link Parameters

Parameter	Description
area-id	Assigns an area ID to the transit area for the virtual link. This ID can be either a decimal value or in dotted-decimal format like a valid IP address. There is no default. The transit area cannot be a stub area.
router-id	Associates a router ID with the virtual link neighbor. The router ID appears in the show ip ospf command display. The router ID is internally derived by each router from the interface IP addresses. Enter this value in the format of an IP address. There is no default.
authentication	(Optional) Specifies an authentication type.
message-digest	(Optional) Specifies the use of message-digest authentication.
null	(Optional) Overrides password or message-digest authentication if configured for the area. No use of authentication.
hello-interval seconds	(Optional) Specifies the time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. An unsigned integer value is advertised in the hello packets. The value must be the same for all attached routers and access servers to a common network. The default is 10 seconds.
retransmit-interval seconds	(Optional) Specifies the time (in seconds) between LSA retransmissions for adjacencies belonging to the interface. Expect round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
transmit-delay seconds	(Optional) Specifies the estimated time (in seconds) to send an LSU packet on the interface. The integer value must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
dead-interval seconds	(Optional) Specifies the time (in seconds) that must pass without hello packets being seen before a neighboring router declares the router down. There is an unsigned integer value. The default is four times the default hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
authentication-key key	(Optional) Specifies the password used by neighboring routers. It is any continuous string of characters up to 8 bytes long that you can enter from the keyboard. This string acts as a key allowing the authentication procedure to generate or verify the authentication field in the OSPF header. Insert this key directly into the OSPF header when originating routing protocol packets. Assign a separate password to each network on a per-interface basis. All neighboring routers on the same network must have the same password to route OSPF traffic. Encrypt the password in the configuration file if the service password-encryption command is enabled. There is no default value.
message-digest-key key-id md5 key	(Optional) Identifies the key and password used by neighboring routers and the router for MD5 authentication. The keyid argument is a number in the range from 1 to 255. The key is an alphanumeric string of up to 16 characters. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. There is no default value.

OSPF Virtual Link Configuration Example 1

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-7

The virtual link command for each router must include the transit area ID and the corresponding virtual link neighboring router ID for you to properly configure a virtual link.

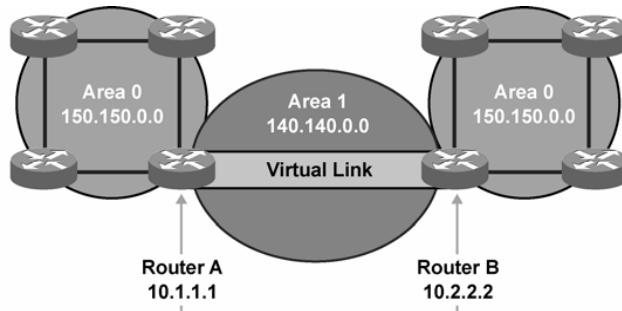
You should always use the **show ip ospf** command on the far-end router to ensure the correct router ID configuration.

In the figure, router 2 builds a virtual link to far-end router 1. Each router points at the other router ID. Remember that the router ID may not refer to the nearest interface. Area 1 is configured as the transit area.

Note Router 2 does not require a **network** command that includes area 0. Router 1 does not include area 3.

OSPF Virtual Link Configuration Example 2

Cisco.com



```
router ospf 1000
network 140.140.0.0 0.0.255.255 area 1
network 150.150.0.0 0.0.255.255 area 0
area 1 virtual-link 10.2.2.2
```

```
router ospf 1000
network 140.140.0.0 0.0.255.255 area 1
network 150.150.0.0 0.0.255.255 area 0
area 1 virtual-link 10.1.1.1
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-8

In the figure, area 0 splits into two pieces due to network failure. A virtual link is used as a backup strategy to temporarily reconnect area 0. Area 1 is used as the transit area.

The show ip ospf virtual-links Command

Cisco.com

```
Router# show ip ospf virtual-links
Virtual Link to router 10.2.2.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 0:00:08 Adjacency State FULL
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-9

You should use the **show ip ospf virtual-links** command to ensure that the configured virtual link works properly. The following table describes the **show ip ospf** command fields shown in the figure in detail.

show ip ospf Fields

Field	Description
Virtual Link to router 10.2.2.2 is up	Specifies the OSPF neighbor and whether the link to that neighbor is up or down
Transit area 0.0.0.1	Specifies the transit area through which the virtual link is formed
via interface Ethernet0	Specifies the interface through which the virtual link is formed
Cost of using 10	Specifies the cost of reaching the OSPF neighbor through the virtual link
Transmit Delay is 1 sec	Specifies the transmit delay on the virtual link
State POINT_TO_POINT	Specifies the state of the OSPF neighbor
Timer intervals configured	Specifies the various timer intervals configured for the link
Hello due in 0:00:08	Specifies when the next hello is expected from the neighbor
Adjacency State FULL	Specifies the adjacency state between the neighbors

Verifying OSPF Virtual Links Operation

This topic explains the **debug ip ospf adj** and **show ip ospf database** commands. These commands are important for understanding the details of a virtual link and for ensuring that the virtual link works properly.

The routers become adjacent and exchange LSAs via the virtual link, similar to a physical link. However, the **show ip ospf neighbor** command does not display neighbor adjacencies over virtual links. The only way to see the neighbor adjacencies is by looking at the router LSA or by using the **debug ip ospf adj** command as the adjacency comes up.

```
R3# debug ip ospf adj
    1w2d: OSPF: Rcv hello from 1.1.1.1 area 0 from OSPF_VL3
    5.0.0.1
    1w2d: OSPF: 2 Way Communication to 1.1.1.1 on OSPF_VL3, state
    2WAY
    1w2d: OSPF: Send DBD to 1.1.1.1 on OSPF_VL3 seq 0xD1C opt 0x62
    flag 0x7 len 32
    1w2d: OSPF: End of hello processing
    1w2d: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL3 seq 0x1617 opt
    0x22 flag 0x7 len 32 mtu 0 state EXSTART
    1w2d: OSPF: First DBD and we are not SLAVE
    1w2d: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL3 seq 0xD1C opt
    0x22 flag 0x2 len 172 mtu 0 state EXSTART
    1w2d: OSPF: NBR Negotiation Done. We are the MASTER
    1w2d: OSPF: Send DBD to 1.1.1.1 on OSPF_VL3 seq 0xD1D opt 0x62
    flag 0x3 len 172
    1w2d: OSPF: Database request to 1.1.1.1
    1w2d: OSPF: sent LS REQ packet to 5.0.0.1, length 36
    1w2d: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL3 seq 0xD1D opt
    0x22 flag 0x0 len 32 mtu 0 state EXCHANGE
    1w2d: OSPF: Send DBD to 1.1.1.1 on OSPF_VL3 seq 0xD1E opt 0x62
    flag 0x1 len 32
    1w2d: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL3 seq 0xD1E opt
    0x22 flag 0x0 len 32 mtu 0 state EXCHANGE
    1w2d: OSPF: Exchange Done with 1.1.1.1 on OSPF_VL3
    1w2d: OSPF: Synchronized with 1.1.1.1 on OSPF_VL3, state FULL
    1w2d: OSPF: Build router LSA for area 0, router ID 3.3.3.3,
    seq 0x80000029
    1w2d: OSPF: Dead event ignored for 1.1.1.1 on demand circuit
    OSPF_VL3

R1# show ip ospf database router 3.3.3.3
    OSPF Router with ID (1.1.1.1) (Process ID 2)
    Router Link States (Area 0)
    Routing Bit Set on this LSA
    LS age: 5 (DoNotAge)
    Options: (No TOS-capability, DC)
    LS Type: Router Links
    Link State ID: 3.3.3.3
    Advertising Router: 3.3.3.3
    LS Seq Number: 80000002
    Checksum: 0x3990
    Length: 36
    Area Border Router
    Number of Links: 1

    Link connected to: a Virtual Link
```

```
(Link ID) Neighboring Router ID: 1.1.1.1
(Link Data) Router Interface address: 6.0.0.3
Number of TOS metrics: 0
    TOS 0 Metrics: 65
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **A virtual link is a feature used to temporarily mend backbone failures.**
- **A virtual link is part of the OSPF standard.**
- **When configuring a virtual link, always use the router ID of the far-end router.**
- **Use the show ip ospf virtual-links command to verify that the virtual link is functioning correctly.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 4-10

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 4-5: Configuring OSPF Virtual Links (Optional)

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) It is acceptable practice to use a virtual link when you want to avoid a tiered backbone in OSPF.
- A) true
 - B) false
- Q2) What are the three reasons for using a virtual link? (Choose three.)
- A) temporary backup purposes
 - B) temporary connection due to network moves or changes
 - C) building a permanent backbone
 - D) backup of a disconnected area 0
- Q3) When you are configuring a virtual link, always use the IP address of the _____.
- A) local router ID
 - B) far-end router ID
 - C) local adjacent interface
 - D) far-end adjacent interface
- Q4) When using the **area area-id virtual link router-id** command, the area ID number that is used is always the transit area.
- A) true
 - B) false

Quiz Answer Key

Q1) B

Relates to: Defining an OSPF Virtual Link

Q2) A, B, D

Relates to: Defining an OSPF Virtual Link

Q3) B

Relates to: Configuring OSPF Virtual Links

Q4) A

Relates to: Verifying OSPF Virtual Links Operation

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:

- Quiz 4-1: OSPF Protocol Overview
- Quiz 4-2: OSPF Packet Types
- Quiz 4-3: Configuring Basic OSPF
- Quiz 4-4: OSPF Network Types
- Quiz 4-5: Types of OSPF Routers and LSAs
- Quiz 4-6: OSPF Route Summarization Techniques
- Quiz 4-7: OSPF Special Area Types
- Quiz 4-8: OSPF Virtual Links

Quiz 4-1: OSPF Protocol Overview

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

Objectives

This assessment tests your knowledge of how to:

- Describe the concept of link-state routing protocol
- Identify the purpose of OSPF areas
- Describe the concept of OSPF adjacencies
- Explain the Open Shortest Path First Shortest Path First calculation

Quiz

Answer these questions:

- Q1) Cisco recommends no more than _____ area or areas per ABR in addition to area 0.
- A) one
 - B) two
 - C) four
 - D) eight
- Q2) An area border router maintains _____.
- A) a separate database for each area it joins
 - B) a single database for all areas
 - C) two databases, one for the backbone, one for all others
 - D) a separate routing table for each area
- Q3) In a multiarea network, any area can be the backbone area, although this is most often area 0.
- A) true
 - B) false
- Q4) When an LSA is received by an OSPF router, it is installed in the:
- A) neighbor table
 - B) topology database (also known as link-state database)
 - C) routing table
- Q5) An OSPF router receives an LSA, the router checks its sequence number, and this number matches the sequence number of the receiving router.
What does the receiving router do with the LSA information?
- A) ignores the LSA
 - B) adds it to the database
 - C) sends newer LSU update to source router
 - D) floods the LSA to the other routers

- Q6) An OSPF router receives an LSA. The router checks its sequence number and finds that this number is *higher* than the sequence number it already recognizes. Which two tasks does the router perform with the LSA information? (Choose two.)
- A) ignores the LSA
 - B) adds it to the database
 - C) sends newer LSU update to source router
 - D) floods the LSA to the other routers
- Q7) An OSPF router receives an LSA. The router checks its sequence number and finds that this number is *lower* than the sequence number it already recognizes. Which two tasks does the router perform with the LSA information? (Choose two.)
- A) ignores the LSA
 - B) adds it to the database
 - C) sends newer LSU update to source router
 - D) floods the LSA to the other routers
- Q8) Each LSA has its own age timer. How long does an LSA wait before requiring an update?
- A) 30 seconds
 - B) 1 minute
 - C) 30 minutes
 - D) 1 hour
- Q9) Distance vector protocols use the concept of split horizon, but link-state routing protocols, such as OSPF, do not.
- A) true
 - B) false
- Q10) The outcome of Dijkstra's calculation is used to populate the _____.
A) topology table
B) routing table
C) neighbor table
D) adjacency table

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-2: OSPF Packet Types

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

Objectives

This assessment tests your knowledge of how to:

- List the types of OSPF packets
- Explain how neighbor adjacencies are established in OSPF
- Identify the exchange process and the neighbor adjacency states of OSPF
- Define OSPF link-state update sequence numbers
- Use the **debug ip ospf packet** command and **debug ip ospf adj** command

Quiz

Answer these questions:

- Q1) OSPF packets are encapsulated in _____.
A) IP using TCP as the transport protocol
B) IP using UDP as the transport protocol
C) IP-only packets
D) Layer 2 frame encapsulation, not IP encapsulation
- Q2) Which OSPF packet type contains information about the hello and dead timer, the area ID, the router priority, DR and BDR IP address, and the stub area flag?
A) hello
B) DBD
C) LSR
D) LSU
- Q3) Which OSPF packet type is used to exchange summary LSA information?
A) hello
B) DBD
C) LSR
D) LSU
- Q4) When do you use a DR?
A) on multiaccess networks to reduce the number of adjacencies required
B) on point-to-point links
C) on all interface types; you always need a DR
D) when you set the link priority to zero
- Q5) In the neighbor list of an Ethernet link, if your router is not the DR and not the BDR, it is a _____.
A) full-state router
B) two-way-state router
C) DROTHER
D) init-state router

- Q6) On a broadcast interface, hello packets are periodically sent every _____.
A) 1 hour
B) 30 minutes
C) 30 seconds
D) 10 seconds
- Q7) What destination address is used when sending an update packet to a DR?
A) 224.0.05
B) 224.0.0.1
C) 255.255.255.255
D) 224.0.0.6
- Q8) The authentication field in an OSPF packet can be set three ways.
Which one of the following methods is NOT correct?
A) no authentication
B) clear-text password
C) triple-DES encryption
D) MD5
- Q9) How long will an LSA stay in the LSDB without receiving a refresh?
A) 1 hour
B) 30 minutes
C) 30 seconds
D) 10 seconds
- Q10) On an LSA, what would be the last sequence number before wrapping to the beginning?
A) 0x80000000
B) 0x7fffffff
C) 0xffffffff
D) 0x80000002

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-3: Configuring Basic OSPF

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

Objectives

This assessment tests your knowledge of how to:

- Configure and verify a basic single-area OSPF configuration
- Use Open Shortest Path First configuration commands to properly enable the OSPF routing process

Quiz

Answer these questions:

- Q1) Which **network** statement is used to configure OSPF on an interface with IP address 172.16.1.1 in area 0?
- A) **network 172.16.0.0 0.0.0.255 area 0**
 - B) **network 172.16.1.1 0.0.0.0 area 0**
 - C) **network 172.16.1.1 255.255.255.255 area 0**
 - D) **network 172.16.0.0 0.0.255.255 area 0**
- Q2) Only one OSPF process can run on a Cisco router at one time.
- A) true
 - B) false
- Q3) Which command is not a valid OSPF **show** command?
- A) **show ip ospf**
 - B) **show ip ospf adjacency**
 - C) **show ip ospf neighbor**
 - D) **show ip ospf interface**
- Q4) The **ospf router-id** command should be used in global configuration mode.
- A) true
 - B) false
- Q5) A router has an Ethernet interface with IP address 172.16.45.1, a loopback 0 interface with IP address 10.3.3.3, a loopback 1 interface with 10.2.2.2, and a **router-id** command with IP address 10.1.1.1.
Which router ID will be selected?
- A) 172.16.45.1
 - B) 10.3.3.3
 - C) 10.2.2.2
 - D) 10.1.1.1

- Q6) The **show ip ospf neighbor** command shows a full state on one of the two neighbors in its table.
Which successfully exchange LSDB information?
- A) neighbor in full state
 - B) neighbor not in full state
 - C) both have exchanged databases
 - D) neither has exchanged databases
- Q7) Which **show** command can be used to verify the OSPF router ID of a router?
- A) **show ip ospf interface**
 - B) **show ip ospf neighbor**
 - C) **show ip ospf**
 - D) **show ip route**
- Q8) When you configure a loopback interface, you choose an IP address that is not going to be advertised by OSPF.
Therefore this loopback address _____.
A) cannot be a router ID because it cannot be pinged
B) can be the router ID, even though it cannot be pinged
C) can be the router ID and can be pinged if a private address is selected
D) cannot be the router ID; you should always advertise loopback addresses
- Q9) Which statement describes the process ID on the **router ospf** command?
- A) All OSPF routers in a network must have the same OSPF process ID.
 - B) The OSPF process ID is an internal number and does not need to match the other router.
 - C) The OSPF process ID is similar to an autonomous system number.
 - D) There can be only one OSPF process ID in a router configuration.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-4: OSPF Network Types

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

Objectives

This assessment tests your knowledge of how to:

- Describe adjacency behavior for a point-to-point link
- Describe adjacency behavior for a broadcast link
- Explain Open Shortest Path First operations over nonbroadcast multiaccess networks
- Identify the different configuration options for Open Shortest Path First over Frame Relay
- Compare common Open Shortest Path First and Frame Relay configuration strategies and examples
- Interpret debug output for IP Open Shortest Path First adjacencies

Quiz

Answer these questions:

- Q1) Which destination IP address does OSPF use when advertising to all SPF routers?
- A) 224.0.0.6
 - B) 224.0.0.5
 - C) 255.255.255.255
 - D) IP address of output interface
- Q2) Which destination IP address does OSPF use when advertising to DRs?
- A) 224.0.0.6
 - B) 224.0.0.5
 - C) 255.255.255.255
 - D) IP address of output interface
- Q3) With a hello interval at 10 seconds, what does the dead interval default to?
- A) 10 seconds
 - B) 20 seconds
 - C) 40 seconds
 - D) 60 seconds
- Q4) The BDR, like the DR, maintains a full set of adjacencies on a broadcast link.
- A) true
 - B) false
- Q5) Which two protocols use the nonbroadcast (NBMA) mode? (Choose two.)
- A) PPP
 - B) HDLC
 - C) X.25
 - D) ATM
 - E) SLIP

- Q6) Which two modes require a DR? (Choose two.)
- A) point-to-point
 - B) broadcast
 - C) point-to-multipoint
 - D) nonbroadcast
- Q7) Which two statements regarding the nonbroadcast (NBMA) mode are correct? (Choose two.)
- A) requires manual **neighbor** router statements
 - B) does not use a DR and BDR
 - C) uses a DR and BDR
 - D) requires multiple subnets
- Q8) When you are using a **neighbor** router statement, you must configure it under the interface.
- A) true
 - B) false
- Q9) Which OSPF modes require **neighbor** statements?
- A) broadcast
 - B) point-to-point
 - C) point-to-multipoint
 - D) point-to-multipoint nonbroadcast
- Q10) You have a partially meshed hub-and-spoke Frame Relay network. You consider using the **ip ospf network broadcast** command on the Frame Relay interface because you do not want to configure **neighbor** router statements.
Is this a good idea?
- A) yes
 - B) no

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-5: Types of OSPF Routers and LSAs

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

Objectives

This assessment tests your knowledge of how to:

- List the types of Open Shortest Path First routers
- Explain, in general terms, all the link-state advertisements defined by Open Shortest Path First, and specifically describe the most common link-state advertisements used in Open Shortest Path First today
- Interpret the Open Shortest Path First link-state database and routing table

Quiz

Answer these questions.

- Q1) Which two LSAs describe intra-area routing information? (Choose two.)
- A) summary
 - B) external 1
 - C) external 2
 - D) router
 - E) network
- Q2) What is the flooding scope of a type 3 LSA?
- A) only within the area it originates from
 - B) within the area it originates plus the backbone area
 - C) within the area it originates plus all other areas
 - D) the backbone area plus all other areas
- Q3) An O E1 route sums up the external metric and the interarea metric, while the O E2 route uses the external metric only. The O E1 route is the default for OSPF; the router must be configured to support O E2.
- A) true
 - B) false
- Q4) The network uses Gigabit Ethernet and you want OSPF to correctly calculate the metric using bandwidth.
Which command should you use to ensure that this happens?
- A) **ip ospf cost** on the interface
 - B) **auto-cost reference-bandwidth** under the OSPF routing process
 - C) **bandwidth** under the interface
 - D) **bandwidth** under the OSPF routing process

- Q5) Looking at the routing table, you notice “[110/55].” What does this mean?
- A) The O E1 cost is 110, and the O E2 cost is 55.
 - B) The AD is 110, and the metric is 55.
 - C) The AD is 55, and the metric is 110.
 - D) The total cost of the route is 165.
- Q6) What does it mean if a router in the routing table has an indicator of O?
- A) It is intra-area.
 - B) It is interarea.
 - C) It is external.
 - D) It is OSPF.
- Q7) What is the difference between an LSA 3 and an LSA 4?
- A) LSA 3 is a summary LSA, and LSA 4 is E1.
 - B) LSA 3 is E1, and LSA 4 is a summary.
 - C) LSA 3 is a summary for networks, and LSA 4 is a summary for ASBRs.
 - D) LSA 3 is a summary for ASBRs, and LSA 4 is a summary for networks.
- Q8) By default, OSPF defines a cost of 1 to a bandwidth of _____.
A) T1
B) 1 Gbps (gigabits per second)
C) 100 Mbps (megabits per second)
D) 10 Gbps
- Q9) The OSPF LSDB shows an LSA with an age of 1799.
What does this mean?
- A) The LSA is going to age out in one more second.
 - B) It has been 1799 minutes since the last update.
 - C) The LSA will be refreshed in one more second.
 - D) The LSA was just refreshed, and another refresh is coming in 29 minutes and 59 seconds.
- Q10) Summary LSAs are not automatically summarized.
- A) true
 - B) false

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-6: OSPF Route Summarization Techniques

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

Objectives

This assessment tests your knowledge of how to:

- Describe route summarization
- Use route summarization commands for Open Shortest Path First
- Use the **default-information originate** command to propagate a default route into Open Shortest Path First
- Identify a default route in Open Shortest Path First

Quiz

Answer these questions:

- Q1) A summary LSA (type 3 LSA) is designed to automatically summarize a network into blocks.
- A) true
B) false
- Q2) When you are configuring route summarization, it is most important to stop which two of the following LSA types from flooding? (Choose two.)
- A) router
B) network
C) summary
D) external
E) NSSA
- Q3) You are at the ABR of area 1 and want to classfully summarize network 172.16.32.0 through 172.16.63.0 into area 0.
Write the configuration command that you would use.

-
- Q4) You are at the ASBR between an OSPF area 0 and an EIGRP network. EIGRP routes are being redistributed into OSPF.

Write the correct summarization command to summarize the EIGRP block 172.16.32.0 through 172.16.63.0.

-
- Q5) It is important to always summarize the routes from area 0 into other areas. Suboptimal path selection can occur if you do not.

- A) true
B) false

- Q6) The **area range** command has an optional parameter called **not-advertise**, which is used to prevent advertising _____.
A) all summary LSAs into area 0
B) summary LSAs that match the **area range** command
C) all external LSAs
D) external LSAs that match the **area range** command
- Q7) Generally, a default route is described in the routing table as an _____.
A) O route
B) O IA route
C) O *E1 route
D) O *E2 route
- Q8) Which command is best to use if you want to establish a default route from a router that has no default route in its routing table?
A) **ip route 0.0.0.0 0.0.0.0 next hop address**
B) **default-information originate**
C) **default-information originate always**
D) **static route**
- Q9) The **area x id range** and **network** commands are similar because both use inverse masks for configuration purposes.
A) true
B) false
- Q10) A default route is a form of route summarization.
A) true
B) false

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-7: OSPF Special Area Types

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

Objectives

This assessment tests your knowledge of how to:

- List the types of Open Shortest Path First areas
- Define and configure Open Shortest Path First stub areas
- Define and configure Open Shortest Path First totally stubby areas
- Define and configure Open Shortest Path First not-so-stubby areas

Quiz

Answer these questions:

- Q1) Which characteristic is not a prerequisite for stub areas?
- A) virtual links not allowed
 - B) ASBRs not allowed
 - C) ABRs not allowed
 - D) one way in and out of the stub area
- Q2) Stub area design will not improve _____.
A) CPU utilization on routers in the stub
B) memory requirements on routers in the stub
C) ability to reach outside networks
D) LSDB size on routers in the stub
- Q3) An LSA type 7 appears in the routing table as an _____.
A) O E1 route
B) O E2 route
C) O N2 route
D) O I/A route
- Q4) What is the difference between stub area and totally stubby area configuration?
A) **no-summary** option at the ABR
B) **area area-id totally-stubby** command at the internal routers
C) **area area-id nssa** command at the internal routers
D) **default-cost** command at the ABR
- Q5) A stub area blocks summary LSAs (type 3 and 4 LSAs).
A) true
B) false

- Q6) Where should you configure the **area area-id stub** command when you are configuring a stub area?
- A) on all routers in the area
 - B) on the ABR
 - C) on the ASBR
 - D) on routers that require stub capability within the area
- Q7) Which two features are specific to Cisco? (Choose two.)
- A) stub areas
 - B) totally stubby areas
 - C) NSSA
 - D) totally stubby NSSA
- Q8) In NSSA, the NSSA ABR translates type 7 LSAs into type 5 LSAs.
- A) true
 - B) false
- Q9) The ABR injects a default route into which three types of areas? (Choose three.)
- A) stub
 - B) totally stubby NSSA
 - C) totally stubby
 - D) area 0
- Q10) Which is the preferred route when you are configuring metrics on a default route?
- A) **area 1 default-cost 100**
 - B) **area 1 default-cost 1**
 - C) **default-metric 100**
 - D) **default-metric 1**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 4-8: OSPF Virtual Links

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

Objectives

This assessment tests your knowledge of how to:

- Define the two major purposes of Open Shortest Path First virtual links
- Configure Open Shortest Path First virtual links
- Verify Open Shortest Path First virtual links operation

Quiz

Answer the following questions:

- Q1) A virtual link is similar to a normal OSPF adjacency because the two routers involved are directly connected to one another.
- A) true
 - B) false
- Q2) When you are configuring a virtual link, which command do you use to find the router ID of the far-end router?
- A) **show ip ospf virtual-links**
 - B) **show ip route**
 - C) **show ip ospf adjacency**
 - D) **show ip ospf**
- Q3) LSAs sent over a virtual link:
- A) do not age out
 - B) use a maximum age of 1 hour
 - C) refresh every 30 minutes
 - D) use a maximum age of 30 minutes
- Q4) A virtual link does not use a hello handshake because of the excessive traffic the hello handshake can cause.
- A) true
 - B) false
- Q5) Which is the proper configuration of a virtual link adjacency state?
- A) exchange
 - B) init
 - C) two-way
 - D) full
- Q6) Virtual links use which network type for the LSDB?
- A) broadcast
 - B) nonbroadcast (NBMA)
 - C) point-to-point
 - D) stub

- Q7) Which three parameters are optional features for the **area virtual-link** command?
(Choose three.)
- A) **hello-interval**
 - B) **router-id**
 - C) **authentication**
 - D) **dead-interval**
- Q8) Under which mode can you configure the **area virtual-link** command?
- A) interface configuration mode
 - B) global configuration mode
 - C) router configuration mode
 - D) area configuration mode
- Q9) Which does a virtual link have as a cost metric by default for the OSPF calculation?
- A) 0
 - B) 1
 - C) 10
 - D) 100
- Q10) The transit area for a virtual link can be a stub area.
- A) true
 - B) false

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 4-1: Open Shortest Path First Protocol Overview

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

Quiz 4-2: Open Shortest Path First Packet Types

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

Quiz 4-3: Configuring Basic Open Shortest Path First

- Q1) B
- Q2) B
- Q3) B
- Q4) B
- Q5) D
- Q6) A
- Q7) A
- Q8) B
- Q9) B

Quiz 4-4: Open Shortest Path First Network Types

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

Quiz 4-5: Types of OSPF Routers and LSAs

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

Quiz 4-6: OSPF Route Summarization Techniques

- Q1) B
- Q2) C, D
- Q3) area 1 range 172.16.0.0 255.255.0.0
- Q4) summary-address 172.16.32.0 255.255.224.0
- Q5) B
- Q6) B
- Q7) D
- Q8) C
- Q9) B
- Q10) A

Quiz 4-7: OSPF Special Area Types

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

Quiz 4-8: OSPF Virtual Links

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

Module 5

Configuring the IS-IS Protocol

Overview

This lesson provides an overview of Intermediate System-to-Intermediate System (IS-IS) Protocol technology structures and protocols, as well as basic configuration examples. IS-IS is a part of the Open Systems Interconnection (OSI) suite of protocols.

The OSI suite uses Connectionless Network Service (CLNS) to provide connectionless delivery of data, and the actual Layer 3 protocol is Connectionless Network Protocol (CLNP). CLNP is the solution for unreliable delivery of data, similar to IP. IS-IS uses CLNS addresses to identify the routers and to build the link-state database (LSDB). An understanding of CLNS address portions is required to configure and troubleshoot IS-IS.

IS-IS operates in strictly CLNS terms; however, Integrated IS-IS supports IP routing as well as CLNS. IS-IS conforms itself to different data-link environments, such as Ethernet and Frame Relay.

Integrated IS-IS is also an IP routing protocol and requires knowledge of the configuration information for Integrated IS-IS in a LAN environment and in a nonbroadcast multiaccess (NBMA) environment.

IS-IS contains the most important characteristics of Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP), because it supports variable-length subnet masking (VLSM) and converges quickly.

Each protocol has advantages and disadvantages, but this commonality makes any of the three scalable and appropriate for supporting the large-scale networks of today.

Module Objectives

Upon completing this module, you will be able to configure Integrated IS-IS on a Cisco router.

Module Objectives

Cisco.com

- Explain the mechanics of IS-IS routing protocol
- Identify elements of an OSI network
- Explain IS-IS operation in a CLNS environment
- Describe integrated IS-IS operation
- Configure integrated IS-IS on a Cisco router

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-2

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- Overview of IS-IS Routing and CLNS
- Understanding CLNS Addressing
- Basic Operations of IS-IS in a CLNS Environment
- Basic Operations of IS-IS in an IP and CLNS Environment
- Configuring Basic IS-IS
- Lesson Assessments

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-3

Overview of IS-IS Routing and CLNS

Overview

This lesson presents a description of Connectionless Network Services (CLNS) and its use with Integrated Intermediate System-to-Intermediate System (IS-IS) Protocol. It describes IS-IS routing and compares IS-IS with OSPF.

Relevance

IS-IS is a proven and extensible IP routing protocol that converges quickly and supports VLSM. IS-IS is a public standard, published as International Organization for Standardization (ISO) 9542 and republished as RFC 995. IS-IS offers support for IP and OSI protocols—called Integrated IS-IS or Dual IS-IS. Although not as common, IS-IS is comparable to, and in some cases preferable to, OSPF.

This lesson addresses some of the concepts necessary to develop an understanding of Integrated IS-IS.

Objectives

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

- Define the uses of IS-IS routing
- Explain how Integrated IS-IS routing operates
- Explain how ES-IS operates
- Differentiate among OSI routing levels
- Compare IS-IS and OSPF routing

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **IS-IS Routing**
- **Integrated IS-IS**
- **ES-IS Protocol Operations**
- **OSI Routing Levels**
- **Comparing IS-IS and OSPF**
- **Summary**
- **Quiz**

IS-IS Routing

IS-IS is the most popular and stable IP routing protocol in the Internet service provider (ISP) industry. The simplicity and stability of IS-IS make it robust in large internetworks. IS-IS is found in large ISPs and in some networks that support OSI protocols. This topic describes some of the basic ways in which IS-IS is used.

Uses of IS-IS Routing

Cisco.com

Large ISPs

- **Simpler implementation than OSPF**
- **Well-positioned for IPv6**
- **Originally deployed by ISPs because U.S. government mandated Internet support of OSI and IP**
- **Stable, no reason to change**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-4

IS-IS development began before development of OSPF. Large ISPs chose IS-IS because of their unique requirement for scalability, convergence, and stability. The U.S. government also required support for OSI protocols in the early Internet. Although this requirement was later dropped, IS-IS solved two problems.

Later, businesses typically chose OSPF because it was a more widely supported native IP protocol. Today it is hard to find information and expertise on IS-IS. Nevertheless, some of the largest networks in the world persist in using IS-IS, which is a tribute to its capabilities.

IS-IS has its own packets; IS-IS information is not carried within another routed protocol. Because IS-IS is protocol-independent, it is capable of supporting IP version 4 (IPv4), IP version 6 (IPv6), or the OSI CLNS protocol.

Integrated IS-IS

This topic provides a brief overview of Integrated IS-IS by discussing the features of the protocol and principles of IS-IS design.

Integrated (or Dual) IS-IS Operation

Cisco.com

IS-IS is designed to do the following:

- **Function as IGP**
- **Have fast convergence**
- **Be stable**
- **Make efficient use of bandwidth, memory, and processor**

IS-IS was originally designed as IGP for the OSI stack of ISO.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-5

ISO specifications refer to routers as intermediate systems (ISs). Thus, IS-IS is a protocol that allows routers to communicate with routers. IS-IS serves as an Interior Gateway Protocol (IGP) for the CLNS, which is part of the OSI family of protocols.

IS-IS was adapted for use with IP, and this version is known as Integrated IS-IS (RFC 1195 and ISO 10589). Integrated IS-IS uses its own packets to transport information between routers, including IP reachability information.

IS-IS routers use IS-IS Hellos (IIHs) to establish and to maintain neighbor relationships. Once the neighbor adjacency is established, IS-IS routers exchange link-state information using link-state packets (LSPs).

IS-IS functions similarly to the way OSPF functions when using stub areas. There is minimal communication of information between areas, which reduces the burden on routers supporting the protocol.

IS-IS Features

Cisco.com

- **Link-state routing protocol**
- **Uses Dijkstra's SPF algorithm**
- **Supports two routing levels:**
 - **Level 1: Builds common topology of system IDs in local area. Routes traffic to other areas through nearest Level 1-2 router.**
 - **Level 2: Exchanges prefix information between areas. Routes traffic to area using lowest-cost path.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

IS-IS is the dynamic link-state routing protocol for the OSI protocol stack. It distributes routing information for routing CLNP data for the ISO CLNS environment.

Integrated IS-IS is an implementation of the IS-IS protocol for routing multiple network protocols. Integrated IS-IS tags CLNP routes with information about IP networks and subnets. Integrated IS-IS provides IP with an alternative to OSPF and combines ISO CLNS and IP routing in one protocol. Integrated IS-IS can be used for IP routing, CLNS routing, or for a combination of the two.

IS-IS operates similarly to OSPF. Both obtain adjacency information using a Hello protocol and distribute a list of neighboring routers for each IS throughout the area as an LSP. Each router then runs Dijkstra's algorithm against its LSDB to pick the best paths.

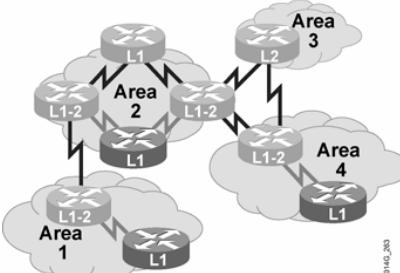
OSI routing takes place at two levels. Level 1 routing within an IS-IS area recognizes the location of the end system (ES) and IS then builds a routing table to reach each system. All devices in a Level 1 routing area have the same area address.

Looking at the locally significant address portion and choosing the lowest-cost path accomplishes routing. If a destination has a different area address, the router sends the traffic to the closest Level 1-2 area border router (ABR).

Level 2 routing learns the locations of Level 1 routing areas and builds an interarea routing table. All ISs in a Level 2 routing area use the destination area address to route traffic using the lowest-cost path.

IS-IS Link-State Operation

Cisco.com



Routers identified as Level 1, Level 2, or Level 1-2:

- **Level 1 routers use LSPs to build topology for local area.**
- **Level 2 routers use LSPs to build topology between different areas.**
- **Level 1 and Level 2 routers act as border routers between Level 1 and Level 2 routing domains.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-7

IS-IS is a link-state protocol that permits partitioning of a routing domain into areas. There are three types of routers as follows:

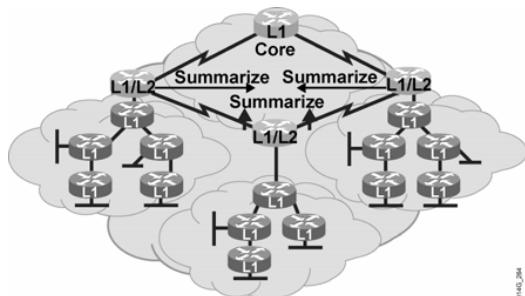
- **Level 1:** Level 1 routers learn about paths within the areas they connect to (intra-area).
- **Level 2:** Level 2 routers learn about paths between areas (interarea).
- **Level 1-2:** Level 1-2 routers learn about paths both within and between areas. Level 1-2 routers are equivalent to ABRs in OSPF.

The path of connected Level 2 and Level 1-2 routers is called the backbone. All areas and the backbone must be contiguous.

Note	Area boundaries fall on the links. Each IS-IS router belongs to exactly one area. Neighboring routers learn whether they are in the same area or different areas and negotiate appropriate adjacencies, Level 1, Level 2, or both.
-------------	--

Integrated IS-IS Design Principles

Cisco.com



- IP and CLNP addresses must be planned.
- Use two-level hierarchy for scalability:
 - Limits LSP flooding
 - Provides opportunity for summarization
- Summarize:
 - Limits update traffic
 - Minimizes router memory and CPU usage

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-8

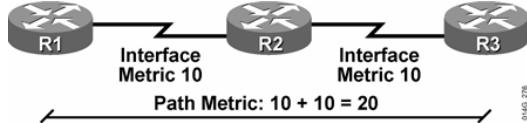
Effective networks are well-planned. The first and most important step in building a scalable network is developing a good addressing plan. Scalability occurs by using route summarization, and route summarization occurs by using hierarchical addressing structure.

Effective address planning presents opportunities to group devices into areas. Using areas confines the scope of LSP propagation and saves bandwidth. Level 1-2 routers, which border a Level 1 area and the Level 2 backbone, are logical places to implement route summarization.

Route summarization saves memory because each IS is no longer responsible for the LSPs of the entire routing domain. Route summarization also saves CPU usage because a smaller routing table is easier to maintain.

Issues with Integrated IS-IS

Cisco.com



- Narrow metrics are limited to 6-bit interface and 10-bit path metric
- Four types of metrics (default, delay, expense, error)
- Cisco IOS software supports only default metric
- Router assigns default metric of 10

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-9

The first issue with IS-IS is that older implementations, those using the narrow metrics, are limited to a maximum interface metric of 63 (6 bits) and a maximum total path metric of 1023 (10 bits). There is little room to distinguish between paths.

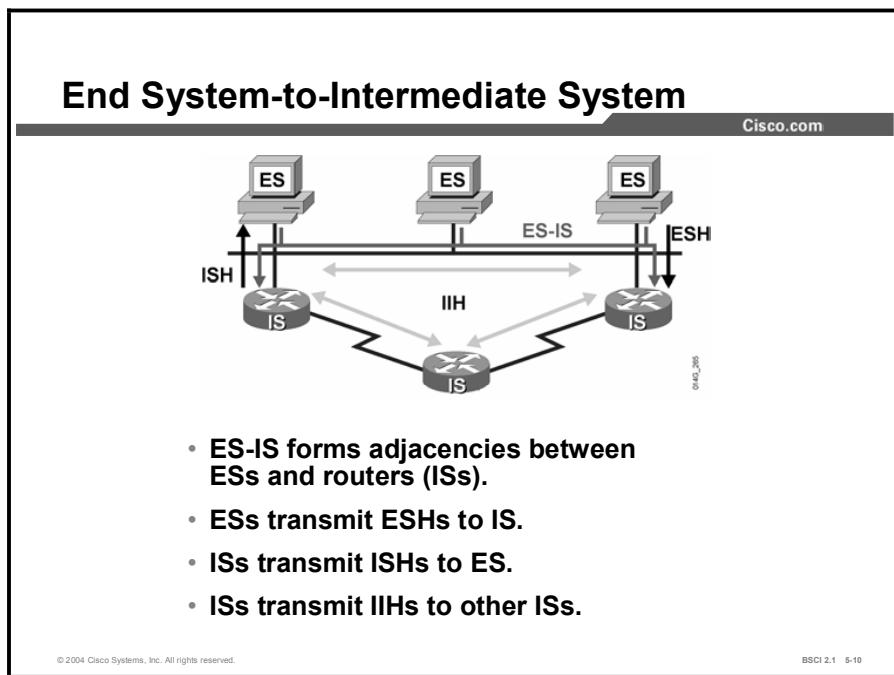
Cisco IOS software, beginning in Software Release 12.0, supports wide metrics that allow a 24-bit interface and 32-bit path metrics. The default, however, is still narrow metrics.

Note You can have complications when you use this new capability if you are working with older routers or with a multivendor environment.

IS-IS, as implemented on Cisco routers, does not automatically scale the interface metric. Instead, all IS-IS interfaces have a default metric of 10, which can be changed manually. If the default metric is not adjusted on each interface, the IS-IS metric becomes similar to the hop count used by Routing Information Protocol (RIP) as the metric.

ES-IS Protocol Operations

End System-to-Intermediate System (ES-IS) Protocol permits ESs and ISs (routers) to discover one another. ES-IS also allows ESs to learn their network-layer addresses. This topic describes how to use ES-IS.



Hosts in the OSI terminology are called *end systems*. ES-IS handles topology information discovery and exchange between ISO ESs (hosts) and ISs (routers).

ESs send End System Hellos (ESHs) to well-known addresses that announce their presence to ISs. Routers listen to ESHs to find the ESs on a segment. Routers include information on ESs in LSPs.

Routers transmit Intermediate System Hellos (ISHs) to well-known addresses, announcing their presence to other ESs. ESs listen for these ISHs and randomly pick an IS to which they forward all their packets. When an ES needs to send a packet to another ES, it sends the packet to one of the router ISs on its directly attached network.

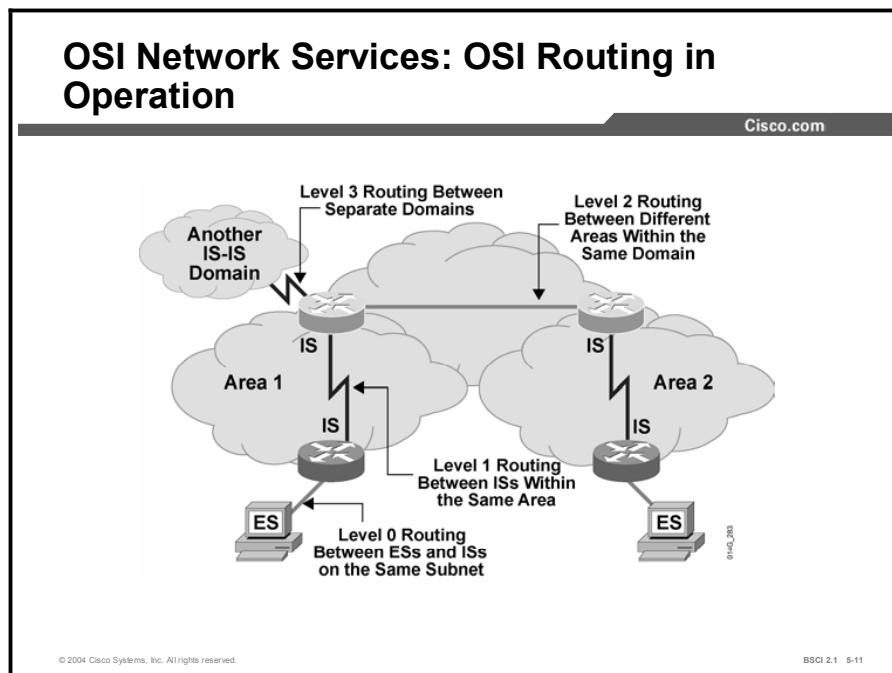
Routers also use IIHs for establishing adjacency between ISs.

IP systems do not use ES-IS. IP has its own processes and applications to handle the same functions as ES-IS, such as Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP).

Although Integrated IS-IS can support IP exclusively, IS-IS still uses CLNS to transmit reachability information and still forms adjacencies using ES-IS.

OSI Routing Levels

The OSI specifications discuss four unique types of routing operations, numbered 0 to 3. This topic discusses how to differentiate among the four OSI routing levels. IS-IS is responsible for Level 1 and Level 2 OSI routing.



IS-IS Level 0 Routing

OSI routing begins when the ESs discover the nearest IS by listening to ISH packets.

ES-IS performs the following tasks:

- Identifies the area prefix to ESs
- Creates adjacencies between ESs and ISs
- Creates data link-to-network address mappings

When an ES needs to send a packet to another ES, it sends the packet to an IS on an attached network. This process is known as Level 0 routing.

IS-IS Level 1 Routing

Each ES and IS resides in a particular area. To pass traffic, the router looks up the destination address and forwards the packet along the best route. If the destination is on the same subnetwork, the IS is aware of the location (from listening to the ESH) and forwards the packet appropriately.

The IS can also provide a redirect message back to the source that tells it that a more direct route is available. If the destination is on a different subnetwork but within the same area, the router identifies the best path using the system ID and forwards the traffic appropriately.

Note Level 1 routing is also called area routing.

IS-IS Level 2 Routing

If a destination address is in another area, the Level 1 IS sends the packet to the nearest Level 2 IS (Level 2 routing). Packet forwarding continues through Level 2 ISs until the packet reaches a Level 2 IS in the destination area. Within the destination area, ISs forward the packet along the best path, based on system ID, until the packet reaches the destination.

Note Level 2 routing is also called interarea routing.

IS-IS Level 3 Routing

Routing between separate domains is called Level 3 routing. Level 3 routing is comparable to Border Gateway Protocol (BGP) interdomain routing in IP. Level 3 routing passes traffic between different autonomous systems. These areas might have different routing logic, and so metrics cannot be directly compared. Level 3 OSI routing is not implemented on Cisco routers, but is specified as being accomplished through the Interdomain Routing Protocol (IDRP).

Summary

- Level 0 routing is conducted by ES-IS.
- Level 1 and Level 2 routing is a function of IS-IS.
- IDRP conducts Level 3 routing. IDRP is similar in purpose to BGP. Cisco Systems routers do not support IDRP.

Comparing IS-IS and OSPF

This topic compares the OSPF and IS-IS protocols, which are link-state IGPs using Dijkstra's algorithm. Most of the development of these two protocols was done concurrently. The work of the development groups produced two protocols that are very similar and are each better because of the other. The practical differences between the two protocols deal with perceived issues of resource usage and customizability.

Integrated IS-IS

Cisco.com

- **Integrated IS-IS is an extended version of IS-IS for mixed ISO CLNS and IP environments.**
- **Integrated IS-IS (RFC 1195) represents an alternative to OSPF in the IP environment.**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 5-12

IS-IS and OSPF share the following critical traits:

- They are open-standard link-state routing protocols.
- They support VLSM.
- They converge quickly.

Most debates of the merits of these protocols are colored by their mutual history; different groups with different cultures developed the protocols.

Digital Equipment Corporation originally developed IS-IS for DECnet Phase V. In 1987, it was selected by the American National Standards Institute (ANSI) to be the OSI IGP. At that time it was capable of routing CLNP only.

The ISO process is an international standards development process. According to an account given by Christian Huitema in his book *Routing in the Internet*, groups within ISO and outside the United States did not approve of TCP/IP because of its origin (it was also called the U.S. Department of Defense protocol).

From the perspective of ISO, IP development was chaotic and imprecise, based on the famous maxim of "loose consensus and running code." From the perspective of the early Internet engineers, the ISO process was slow, irritating, and disenfranchising.

In 1988, the U.S. National Science Foundation Network (NSFnet) was created. The IGP used was based on an early draft of IS-IS. The extensions to IS-IS for handling IP were developed in 1988. OSPF development began during this time, and was loosely based on IS-IS.

In 1989, OSPF version 1 (OSPF v1) was published, and conflict ensued between the proponents of IS-IS and OSPF. The Internet Engineering Task Force (IETF) eventually supported both, although it continued to favor OSPF. With the unofficial endorsement of the IETF, OSPF eventually became the more popular.

By the mid-1990s, large ISPs in need of an IGP selected IS-IS for two reasons. First, IS-IS supported both CLNS and IP, which solved two problems at once. Second, OSPF was seen as immature at the time.

Similarities between IS-IS and OSPF

Cisco.com

- Integrated IS-IS and OSPF are both link-state protocols with the following similar features:
 - Link-state representation, aging, and metrics
 - LSDBs and SPF algorithms
 - Update, decision, and flooding processes
- Scalability of link-state protocols has been proven (ISP backbones)
- Convergence capabilities are similar (same algorithm)

©2004 Cisco Systems, Inc. All rights reserved.

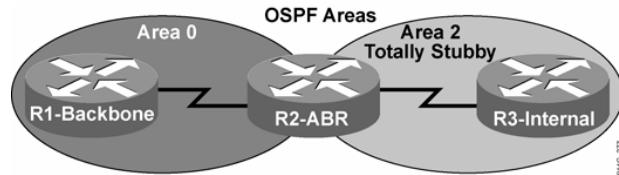
BSCI 2.1 5-13

IS-IS and OSPF are more similar than dissimilar. Both routing protocols have the following characteristics:

- They are link-state routing protocols.
- They use similar mechanisms (link-state advertisements [LSAs], link-state timers, and database synchronization) to maintain the health of the LSDB.
- They are successful in the largest and most demanding deployments (ISP networks).
- They converge quickly after network changes.

Integrated IS-IS vs. OSPF: Area Design

Cisco.com



- **OSPF is based on a central backbone with all other areas attached to it.**
 - In OSPF the border is inside routers (ABRs).
 - Each link belongs to one area.

© 2004 Cisco Systems, Inc. All rights reserved.

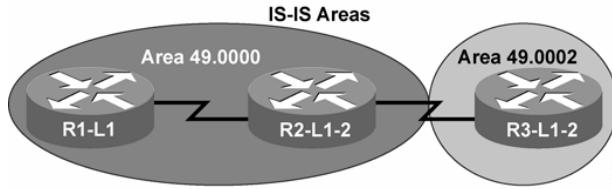
BSCI 2.1 5-14

Certain design constraints exist because the configuration of OSPF is based on a central backbone, area 0, with all other areas being physically attached to area 0.

When you use this type of hierarchical model, a consistent IP addressing structure is necessary to summarize addresses into the backbone. This type of hierarchical model also reduces the amount of information carried in the backbone and advertised across the network.

Integrated IS-IS vs. OSPF: Area Design (Cont.)

Cisco.com



In IS-IS the area borders lie on links.

- Each IS-IS router belongs to exactly one area.
- IS-IS is more flexible when extending the backbone.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-18

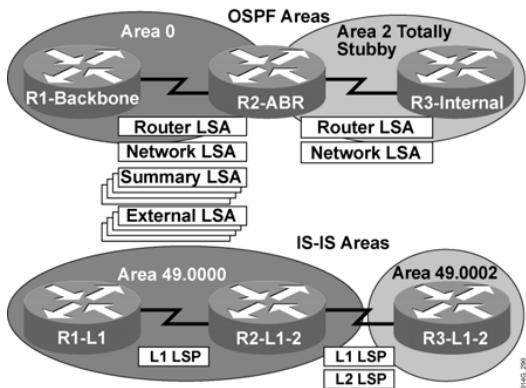
In comparison, IS-IS has a hierarchy with Level 1 and Level 2 or Level 1-2 routers, and the area borders lie on links. However, significantly fewer LSPs are used; therefore, more routers, at least 1000, can reside in a single area.

This capability makes IS-IS more scalable than OSPF. IS-IS permits a more flexible approach to extending the backbone.

The backbone can be extended by simply adding more Level 2 and Level 1-2 routers, a less complex process than with OSPF.

Advantages of IS-IS

Cisco.com



- Supports OSI and TCP/IP
- More extensible through TLV design

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-16

The differences between OSPF and IS-IS are small; however, they do exist. OSPF produces many small advertisements. IS-IS updates are grouped by the router and sent as one LSP. Thus, as network complexity increases, the update packet size is not an issue. Each packet must be routed, though, and routing takes network resources; so more packets represent a larger impact on the network. OSPF runs on top of IP, whereas IS-IS runs through CLNS.

IS-IS is also more efficient than OSPF in the use of CPU resources and in the way it processes routing updates. Not only are there fewer LSPs to process (LSAs, in OSPF terminology) but also the mechanism by which IS-IS installs and withdraws prefixes is less intensive because it revolves around network entity title (NET) addresses, which are already heavily summarized.

Both OSPF and IS-IS are link-state protocols and thus provide fast convergence. The convergence time depends on a number of factors, such as timers, number of nodes, and type of router. Based on the default timers, IS-IS detects a failure faster than OSPF; therefore, convergence occurs more rapidly. If there are many neighboring routers and adjacencies, the convergence time may also depend on the processing power of the router. IS-IS is less CPU-intensive than OSPF.

The IS-IS default timers permit more tuning than OSPF. There are more timers to adjust; therefore, you can achieve finer granularity. If you turn the timers, convergence time decreases significantly. However, it is important to note that stability can be affected by this speed.

New ideas are not easily expressed in OSPF packets and require the creation of a new LSA. The OSPF description schema is difficult to extend, because of compatibility issues and because it was developed exclusively for IP version 4 (IPv4). IS-IS is easy to extend through the Type, Length, Value (TLV) mechanism. TLV strings, called *tuples*, encode all IS-IS updates. IS-IS can easily grow to cover IP version 6 (IPv6) or any other protocol, because extending IS-IS consists simply of creating new type codes.

Advantages of OSPF

Cisco.com

- **OSPF has more features, as follows:**
 - Has three area types: normal, stub, and NSSA
 - Defaults to scaled metric (IS-IS always 10)
- **OSPF is supported by many vendors.**
- **Information, examples, and experienced engineers are easier to find.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-17

A company may choose OSPF over IS-IS because OSPF is more optimized and was designed exclusively as an IP routing protocol.

Networking equipment must support OSPF and network engineers must be familiar with OSPF theory and operation. It is relatively easy to find equipment and personnel to support an OSPF infrastructure. Furthermore, OSPF documentation is much more readily available than documentation for IS-IS.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **IS-IS is the most popular and stable IP routing protocol in the ISP industry.**
- **IS-IS allows routers to communicate with routers and serves as an IGP for the CLNS.**
- **ES-IS permits ESs and ISs to discover one another.**
- **OSI specifies four unique types of routing operations, numbered 0 to 3.**
- **IS-IS and OSPF are both open standards, support VLSM, and converge quickly.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-18

References

For additional information, refer to these resources:

- RFC 995, *End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8437*.
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.
- Martey, A. *IS-IS Network Design Solutions*. Indianapolis, Indiana: Cisco Press; 2002.

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 protocols does IS-IS support? (Choose two.)

- A) TCP/IP
- B) IPX
- C) OSI CLNS
- D) AppleTalk

Q2) Which two characteristics describe IS-IS? (Choose two.)

- A) It is an Interior Gateway Protocol (IGP).
- B) It is an Exterior Gateway Protocol (EGP).
- C) It is efficient in its use of network resources.
- D) It is an advanced distance vector routing protocol.

Q3) Which two types of levels does IS-IS use to support routing? (Choose two.)

- A) Level 1 for IP
- B) Level 1 for interarea routing
- C) Level 2 for interarea routing
- D) Level 2 for CLNS
- E) Level 0 for interdomain routing
- F) Level 1 for intra-area routing
- G) Level 2 for intra-area routing

Q4) Which of the following is ES-IS responsible for?

- A) Level 0 routing
- B) Level 1 routing
- C) Level 2 routing
- D) Level 3 routing

Q5) Which two of the following are IS-IS responsible for? (Choose two.)

- A) Level 0 routing
- B) Level 1 routing
- C) Level 2 routing
- D) Level 3 routing

Q6) Routing between areas is described as which of the following?

- A) Level 0 routing
- B) Level 1 routing
- C) Level 2 routing
- D) Level 3 routing

Q7) Check the characteristics that can be attributed to IS-IS and those that can be attributed to OSPF. Some characteristics may apply to both.

	IS-IS	OSPF
Link-state protocol		
Fast convergence		
Supports VLSM		
More extensible		
Documentation and experienced engineers easy to find		
Most customized to IP		
Metrics scale automatically		

Quiz Answer Key

Q1) A, C

Relates to: IS-IS Routing

Q2) A, C

Relates to: Integrated IS-IS

Q3) F, G

Relates to: Integrated IS-IS

Q4) A

Relates to: OSI Routing Levels

Q5) B, C

Relates to: OSI Routing Levels

Q6) C

Relates to: OSI Routing Levels

Q7)

	IS-IS	OSPF
Link-state protocol	X	X
Fast convergence	X	X
Supports VLSM	X	X
More extensible	X	
Documentation and experienced engineers easy to find		X
Most customized to IP		X
Metrics scale automatically	X	

Relates to: Comparing IS-IS and OSPF

Understanding CLNS Addressing

Overview

This lesson defines Connectionless Network Service (CLNS) addressing and identifies particular address portions; such as network service access points (NSAPs).

Relevance

Unlike IP addresses, CLNS addresses apply to entire nodes and not to interfaces. Because IS-IS was originally designed for CLNS, IS-IS requires CLNS node addresses to function properly.

CLNS addresses used by routers are called NSAPs. One part of an NSAP address is the NSAP selector (NSEL) byte. When an NSAP is specified with an NSEL of 0, then the NSAP is called the network entity title (NET). An NSEL of 0 identifies network services.

This lesson defines NSAP and NET addresses for use with Integrated IS-IS.

Objectives

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

- Define the NSAP address
- Define the NET address

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **NSAP Addresses**
- **NET Addresses**
- **Summary**
- **Quiz**

NSAP Addresses

NSAP addresses have a maximum size of 20 bytes. This topic describes the various NSAP uses that require definition of different address structures. The high-order bits describe interarea structure, and the low-order bits identify unique systems within an area.

OSI Address Assignment

Cisco.com

- **OSI network-layer addressing is implemented with NSAP addresses.**
- **The NSAP address identifies any system in the OSI network.**
- **Various NSAP formats are used in various systems, because different protocols may use different representations of NSAP.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-4

Link-state advertisements (LSAs), which are also called link-state packets (LSPs), Hello protocol data units (PDUs), and other routing PDUs are OSI-format PDUs; therefore, every IS-IS router requires an OSI address.

These IS-IS PDUs are encapsulated directly into an OSI data-link frame. There is no Connectionless Network Protocol (CLNP) header and no IP header.

IS-IS uses the OSI address in the LSPs to identify the router and build the topology table and the underlying IS-IS routing tree.

OSI addresses, or NSAPs, contain the following:

- OSI address of the device
- Link to the higher-layer process

The NSAP address is equivalent to the combination of the IP address and upper-layer protocol in an IP header.

IS-IS NSAP Address Structure

Cisco.com



- The Cisco implementation of Integrated IS-IS distinguishes only the following three fields in the NSAP address:
 - Area address: Variable-length field (1 to 13 octets) composed of high-order octets, excluding system ID and SEL.
 - System ID: ES or IS identifier in an area; fixed length of six octets in Cisco IOS software.
 - NSEL: One octet NSAP selector, service identifier.
- Total length of NSAP is from 8 (minimum) to 20 octets (maximum).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

The Cisco implementation of Integrated IS-IS divides the NSAP address into three fields: the area address, the system ID, and the NSEL. However, Cisco routers routing CLNS data use addressing that conforms to the ISO 10589 standard. ISO NSAP addresses consist of the following:

- The initial domain identifier (IDI) identifies the domain of the NSAP address. The authority and format identifier (AFI) and IDI make up the initial domain part (IDP) of the NSAP address. The IDP corresponds roughly to an IP classful major net.
- The AFI byte specifies the format of the address and the authority that assigned that address. Some valid values include are shown in the table.

AFI Value	Address Domain
39	ISO Data Country Code (DCC)
45	E.164
47	ISO 6523 International Code Designator (ICD)
49	Locally administered (private)

- The IDI identifies a subdomain under the AFI. For instance, 47.0005 is assigned to civilian departments of the U.S. government, and 47.0006 to the U.S. Department of Defense.
- The domain specific part (DSP) contributes to routing within an IS-IS routing domain. The high-order domain specific part (HO-DSP), system ID, and NSEL make up the DSP of the NSAP address.
- The HO-DSP subdivides the domain into areas. The HO-DSP is more or less the OSI equivalent of a subnet in IP.
- The system ID identifies an individual OSI device. In OSI, a device has an address, just as it does in DECnet, while in IP, each interface has an address.
- The NSEL identifies a process on the device and corresponds roughly to a port or socket in IP. The NSEL is not used in routing decisions.

Typical NSAP Address Structure

Cisco.com

The simplest NSAP format used by most companies running IS-IS as their IGP is as follows:

- AFI set to 49
 - Locally administered means you can assign your own addresses
- Area ID
 - Must be at least 1 byte
- System ID
 - Cisco routers require a 6-byte system ID
- NSEL
 - Always set to 0 for a router

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

The simplest NSAP format, when using IS-IS as an Interior Gateway Protocol (IGP), is as follows:

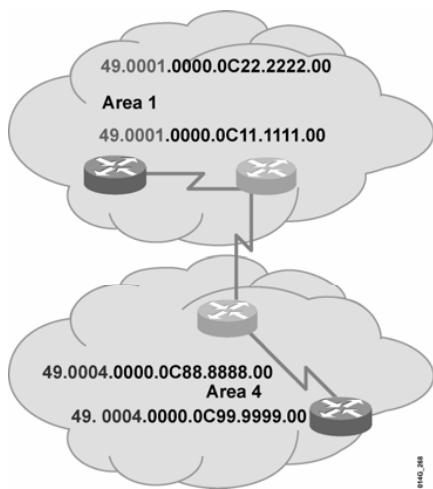
- AFI set to 49, which signifies that the AFI is locally administered and individual addresses can be assigned
- The area identifier (ID), which must be at least 1 byte
- System ID; Cisco routers compliant with the U.S. Government OSI Profile (GOSIP) version 2.0 standard require a 6-byte system ID
- NSEL, which must always be set to 0 for a router

For example, you might assign 49.0001.0000.0c12.3456.00, which represents the following:

- AFI of 49
- Area ID of 0001
- System ID of 0000.0c12.3456, MAC address of a LAN interface
- NSEL of 0. The NSAP is called the NET when it has an NSEL of 0. Routers use the NET to identify themselves in the IS-IS PDUs.

Identifying Systems in IS-IS

Cisco.com



The area address uniquely identifies the routing area, and the system ID identifies each node.

- All routers within an area must use the same area address.
- An ES may be adjacent to a Level 1 router only if they share a common area address.
- Area address is used in Level 2 routing.

©2004 Cisco Systems, Inc. All rights reserved.

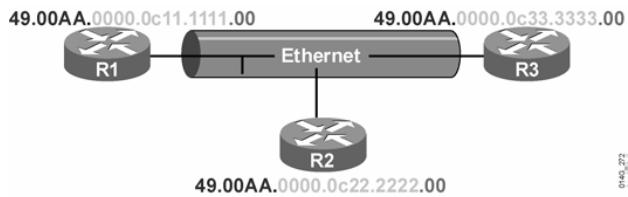
BSCI 2.1 5-7

The first part of a NET is the area ID. The area ID is associated with the IS-IS routing process. Unlike OSPF, an IS-IS router can be a member of only one area. Other address restrictions are as follows:

- All routers in an area must use the same area address, which actually defines the area.
- ESs recognize only ISs and other ESs on the same subnetwork that share the same area address.
- Level 1 intra-area routing is based on system IDs. Therefore, each ES and IS must have a unique system ID within the area.
- All Level 2 ISs eventually recognize all other ISs in the Level 2 backbone. Therefore, they must also have unique system IDs.

Identifying Systems in IS-IS: System ID

Cisco.com



- **System ID is the address used to identify the IS; it is not just an interface. Cisco supports only a 6-byte system ID.**
- **System ID is used in Level 1 routing and has to be unique within an area.**
- **System ID has to be unique within Level 2 routers that form the routing domain.**
- **General recommendation: domain-wide unique system ID**
 - **May be MAC (for example, 0000.0c12.3456) or IP address (for example, 1921.6800.0001) taken from an interface**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-8

The low-order 6 bytes of an NSAP are the system ID. The system ID must be unique within an area. It is customary to use a MAC address from the router, or, for Integrated IS-IS, to code an IP address into the system ID.

System IDs should remain unique across the domain. If the system IDs remain unique, there can never be a conflict at Level 1 or Level 2 if, for example, a device moves into a different area.

All of the system IDs in a domain must be of equal length. Cisco enforces this OSI directive by fixing the length of the system ID at 6 bytes in all cases.

NET Addresses

This topic identifies the features of NET addresses. NET addresses are NSAP addresses with an NSEL value of 0. A NET address is used to uniquely identify an OSI host within an IS-IS routing domain. Because IS-IS originates from the OSI world, NET addresses are required even if the only routed protocol is IP.

OSI Addressing: NET

Cisco.com

- **NSAP: Address at the network layer that includes a service identifier (protocol number)**
- **NET: NSAP with a service identifier of 00**
 - Used in routers because they implement the network layer only (base for SPF calculation)
- **The official NSAP prefixes are required for CLNS routing: AFI 49 denotes private address space**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-9

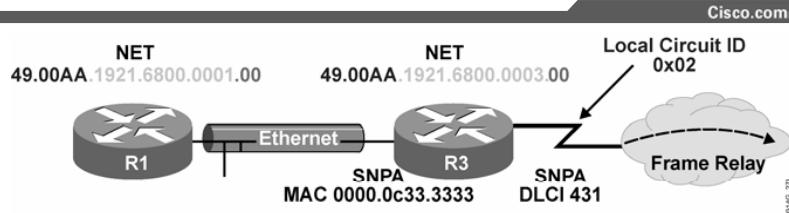
If the upper-layer process ID (NSEL) is 00, then the NSAP refers to the device itself; that is, it is the equivalent of the Layer 3 OSI address of that device. The Layer 3 OSI address is known as the NET.

Routers use the NET to identify themselves in the LSPs and, therefore, to form the basis for the OSI routing calculation.

Addresses starting with the AFI value of 49 are private addresses, analogous to RFC 1918 for IP addresses. IS-IS routes these addresses. However, this group of addresses should not be advertised to other CLNS networks because they are ad hoc addresses. Other companies that use a value of 49 may have created different numbering schemes that, when used together, could create confusion.

Addresses starting with AFI values 39 and 47 represent the ISO DCC and ISO ICD, respectively.

Identifying Systems: Subnetwork and Circuit



SNPA identified by:

- Encapsulation type or DLCI address on point-to-point interfaces (HDLC, Frame Relay)
- MAC address on LAN interfaces (0000.0c12.3456)

Interfaces uniquely identified by circuit ID:

- One octet number on point-to-point interfaces (like 0x00)
- Circuit ID concatenated with 6-octet system ID of a designated router on broadcast multiaccess networks to form 7-octet LAN ID (1921.6800.0001.01)

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-10

Additional IS-IS terms include:

- The subnetwork point of attachment (SNPA) is the point that provides subnetwork services. SNPA is the equivalent of the Layer 2 address corresponding to the Layer 3, NET, or NSAP address and is usually a MAC address on a LAN or a virtual circuit ID in X.25, Frame Relay, or ATM.
- A circuit is the IS-IS term for an interface. NSAP and NET refer to the entire device, so a circuit ID is used to distinguish a particular interface.

A link is the path between two neighbor ISs and is defined as being up when communication is possible between the two neighbor SNPAs.

The SNPA is taken from the following:

- The MAC address on a LAN interface.
- The virtual circuit ID from X.25 or ATM and the data-link connection identifier (DLCI) from Frame Relay.
- For High-Level Data Link Control (HDLC) interfaces, the SNPA is simply HDLC.

The circuit ID allows interfaces and networks to be distinguished by the router. The router assigns a circuit ID (one octet) to each interface on the router as follows:

- In the case of point-to-point interfaces, the SNPA is the sole identifier for the circuit. For example, on an HDLC point-to-point link, the circuit ID is 0x00.
- In the case of LAN interfaces, the circuit ID is tagged to the end of the system ID of the designated IS to form a 7-byte LAN ID, for example, 1921.6800.0001.01. On Cisco routers, the router host name is used instead of the system ID; therefore the circuit ID of a LAN interface may look like "P6R4.01."

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Various uses of NSAP addresses require definition of different address structures:**
 - High-order bits describe interarea structure
 - Low-order bits identify unique systems within an area
- **NET addresses are NSAP addresses with an NSEL value of 0.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-11

References

For additional information, refer to these resources:

- RFC 995, *End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8437*.
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.
- Martey, A. *IS-IS Network Design Solutions*. Indianapolis, Indiana: Cisco Press; 2002.

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) Put the parts of an NSAP address in the correct order.

- A) system ID
- B) HO-DSP
- C) AFI
- D) NSEL
- E) IDI

Q2) Which component does an NSAP address identify?

- A) interface
- B) device
- C) process
- D) protocol

Q3) Which characteristic describes a NET?

- A) always has an AFI of 49
- B) always has a 3-byte HO-DSP
- C) always has an NSEL of 00
- D) is never assigned to a router

Q4) Which prefix does private AFI use?

- A) 49.0001
- B) 37
- C) 47
- D) 49
- E) 37.1921

Quiz Answer Key

- Q1) 1-C, 2-E, 3-B, 4-A, 5-D
Relates to: NSAP Addresses
- Q2) B
Relates to: NSAP Addresses
- Q3) C
Relates to: NET Addresses
- Q4) D
Relates to: NET Addresses

Basic Operations of IS-IS in a CLNS Environment

Overview

This lesson introduces the concepts used by Intermediate System-to-Intermediate System (IS-IS) in a Connectionless Network Service (CLNS) environment, the first step to understanding Integrated IS-IS.

Relevance

IS-IS runs directly on the data-link layer and does not use IP or CLNS as a network protocol. IS-IS is similar to OSPF in the following ways:

- It supports different media in different ways.
- It recognizes neighbors and advertises links to build a link-state table.

This lesson describes how CLNS addressing affects IS-IS operation. In addition, this lesson describes how the IS-IS protocol learns topology, makes routing decisions, and handles different data links.

Objectives

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

- Contrast intra-area and interarea routing in a CLNS environment
- Explain router level definitions
- Identify uses of IS-IS PDUs
- Identify uses of LSPs
- List the network topologies supported by IS-IS
- Describe adjacency behavior in a broadcast network
- Compare LAN, WAN, and Level 2 adjacencies
- Identify the types of LSDB synchronization

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Intra-Area and Interarea Addressing and Routing**
- **IS-IS Routing Levels**
- **IS-IS Protocol Data Units**
- **Link-State Packets**
- **Topologies**
- **Broadcast Networks**
- **Point-to-Point Networks**
- **Link-State Database Synchronization**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 5-3

Intra-Area and Interarea Addressing and Routing

This topic identifies the features of intra-area and interarea addressing. IS-IS routing flows naturally from the OSI address plan. Areas are identified and unique system IDs are given to each device.

Addressing and Routing

Cisco.com

- **Communication is only between an ES and IS in the same area.**
- **Area portion is used to route between areas.
System ID is not considered.**
- **System ID is used to route within an area.
Area ID is not considered.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-4

An OSI NSAP address can be up to 20 octets long. The final byte is the selector byte, the preceding six bytes are the system ID, and the leading bytes are the area ID. The system ID can be set to any arbitrary value. However, it must be unique within the routing area, and it is recommended that every system ID be globally unique.

The area ID can range from 1 to 13 bytes in length, as specified by the ISO standard. Therefore, an NSAP for an IS-IS network can be as little as 8 bytes in length. However, the NSAP is usually longer to permit some granularity in the allocation of areas. The area ID prefix is common to all devices in an area and unique for each area. Sets of ISs and ESs are in the same area if they share the same area ID.

Routing within an area involves collecting system IDs and adjacencies for all ISs and ESs in an area and using Dijkstra's algorithm to compute best paths between devices. Level 1 routers are aware only of the local area topology. They pass the traffic bound outside the area to the closest Level 1-2 area border router (ABR).

Routing between areas is based on area ID. Level 2 routers in different areas exchange area ID information and use Dijkstra's algorithm to compute best paths between areas. They pass traffic between areas to the closest Level 1-2 ABR.

OSI IS-IS Routing Logic

Cisco.com

Level 1 router: For a destination address, compare the area ID to this area.

- If not equal, pass to nearest Level 1-2 router.
- If equal, use Level 1 database to route by system ID.

Level 1-2 router: For a destination address, compare the area ID to this area.

- If not equal, use Level 2 database to route by area ID.
- If equal, use Level 1 database to route by system ID.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

When an ES is required to send a packet to another ES, the packet goes to one of the ISs on a network directly attached to the ES. The router then searches for the destination address and forwards the packet along the best route.

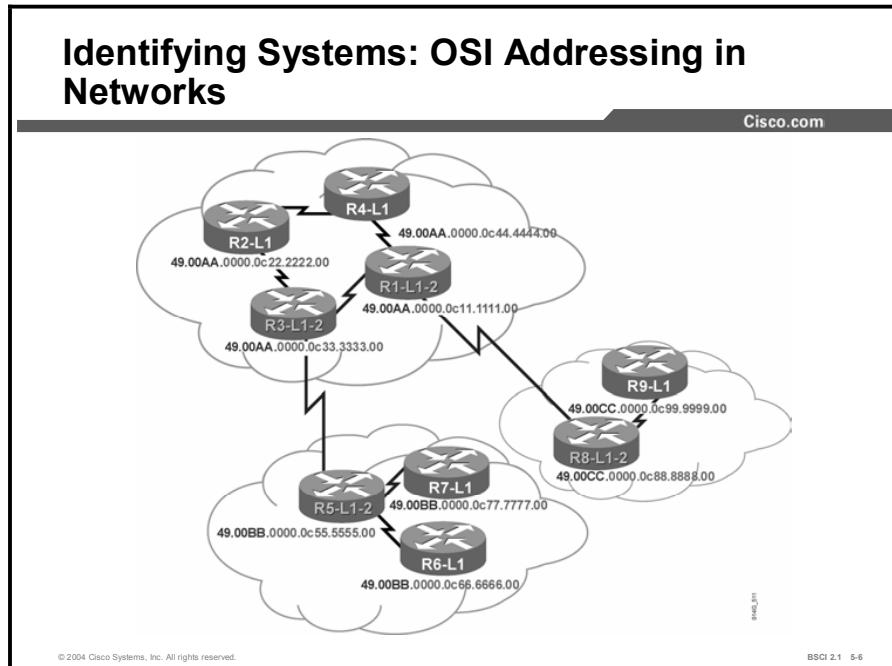
If the destination ES is in the same area, the local IS recognizes the location by listening to End System Hello (ESH) packets and forwards the packet appropriately.

If the destination address is an ES in another area, the Level 1 IS sends the packet to the nearest Level 1-2 IS. Forwarding through Level 2 ISs continues until the packet reaches a Level 2 IS in the destination area.

Within the destination area, ISs forward the packet along the best path until the destination ES is reached.

Because each router makes its own best-path decisions at every hop along the way, there is a significant chance that paths will not be reciprocal. That is, return traffic can take a different path than the outgoing traffic. For this reason, it is important to know the traffic patterns within your network and tune IS-IS for optimal path selection if necessary.

Example



Consider traffic from router 7 to router 9:

1. Router 7 recognizes that the prefix (49.00CC) of router 9 is not the same as the prefix (49.00BB) of router 7. Router 7 therefore passes the traffic to the closest Level 1-2 ABR, router 5. Router 7 uses its Level 1 topology database to find the best path to router 5.
2. Router 5 uses its Level 2 topology database to pick the best next hop to reach the prefix 49.00CC: router 3. Router 5 does not use the destination system ID in this decision.
3. Router 3 uses its Level 2 topology database to pick the best next hop to reach the prefix 49.00CC: router 1. Router 3 does not use the destination system ID in this decision.
4. Router 1 uses its Level 2 topology database to pick the best next hop to reach the prefix 49.00CC: router 8. Router 1 does not use the destination system ID in this decision.
5. Router 8 recognizes that the prefix (49.00CC) of router 9 is the same as the prefix (49.00CC) of router 8. Router 8 therefore passes the traffic to router 9 using its Level 1 topology database to find the best path.

IS-IS Routing Levels

This topic identifies the different routing levels associated with IS-IS.

Level 1, Level 2, and Level 1-2 Routers

Cisco.com

Level 1 (like OSPF internal nonbackbone routers):

- Intra-area routing enables ES to communicate.
- Level 1 area is a collection of Level 1 and Level 1-2 routers.
- It keeps copy of the Level 1 area LSDB.

Level 1-2 (like OSPF ABR):

- Intra-area and interarea routing.
- Keeps separate Level 1 and Level 2 LSDBs and advertises default route to Level 1 routers.

Level 2 (like OSPF backbone routers):

- Interarea routing.
- Level 2 (backbone area) is a contiguous set of Level 1-2 and Level 2 routers.
- Keeps a copy of the Level 2 area LSDB.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-7

IS-IS is a link-state protocol that permits partitioning of a routing domain into areas. Routers (ISs) are of two types: Level 1 and Level 2.

- Level 1 routers recognize paths within the areas to which they are connected (intra-area).
- Level 2 routers learn about paths among areas (interarea).

A router can be Level 1 or Level 2, or it can be both Level 1 and Level 2 (Level 1-2).

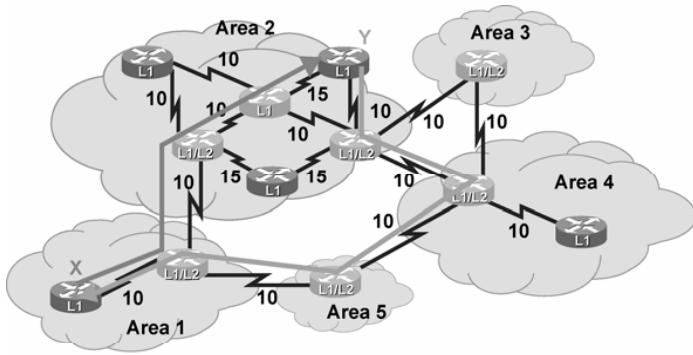
The path of connected Level 2 and Level 1-2 routers is called the backbone. All areas and the backbone must be contiguous.

Note

Area boundaries fall on the links. Neighboring routers recognize whether they are in the same or different areas and negotiate appropriate adjacencies (Level 1, Level 2, or both).

OSI Area Routing

Cisco.com



What path would X use to reach Y?
What path would Y use to reach X?

642

In the figure, area 1 contains two routers:

- One router borders area 2 and is a Level 1-2 IS.
 - The other router is contained within the area and is a Level 1 only.

Area 2 has many routers:

- A selection of routers is specified as Level 1. The routers route either internally to that area or to the exit points.
 - Level 1-2 routers form a chain across the area linking to the neighbor areas. Although the middle router of the three Level 1-2 routers does not link directly to another area, the middle router must support Level 2 routing to ensure the backbone is contiguous. If the middle router fails, the other Level 1-only routers cannot perform the Level 2 function (despite providing a physical path across the area), and the backbone is broken.

Area 3 contains one router that borders areas 2 and 4, yet it has no intra-area neighbors and is performing Level 2 functions only. If you add another router to area 3, the border router reverts to Level 1-2 functions.

In the figure shown, the border between the areas in an IS-IS network is the link between Level 2 routers. (This example is in contrast to OSPF, where the border exists inside the ABR itself.)

In the figure, symmetric routing cannot occur because Level 2 details are hidden from Level 1 routers, which recognize only a default route to the nearest Level 1-2 router.

Traffic from router X to router Y flows from router X to its closest Level 1-2 router. The Level 1-2 router then forwards the traffic along the shortest path to the destination area (area 2). Once the traffic flows into area 2, the traffic is routed along the shortest intra-area path to router Y.

Router Y routes return packets to router X to its nearest Level 1-2 router. The Level 1-2 router recognizes the best route to area 1 via area 4, based on the lowest-cost Level 2 path.

Because Level 1 and Level 2 computations are separate, the path taken from router Y back to router X is not the least-cost option from router Y to router X.

Asymmetric routing (packets taking different paths in different directions) is not detrimental to the network. However, this type of routing can make troubleshooting difficult and is sometimes a symptom of suboptimal design. Like EIGRP and OSPF, a good IS-IS design is generally hierarchical.

A feature available since Cisco IOS Software Release 12.0 allows Level 2 routes to leak in a controlled manner to Level 1 routers, which helps avoid asymmetric routing.

IS-IS Protocol Data Units

This topic describes the four types of PDUs. IS-IS PDUs are encapsulated directly into an OSI data-link frame. There is no CLNP and IP header.

OSI IS-IS PDUs

Cisco.com

- **IS-IS PDUs are encapsulated directly into a data-link frame. There is no CLNP or IP header in a PDU.**
- **IS-IS PDUs are as follows:**
 - Hello (ESH, ISH, IIH)
 - LSP (nonpseudonode and pseudonode)
 - PSNP (partial sequence number PDU)
 - CSNP (complete sequence number PDU)

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 5-9

IS-IS has the following four types of PDUs:

- **Hello PDU (ESH, Intermediate System Hello [ISH], IS-IS Hello [IIH]):** Used to establish and maintain adjacencies
- **Link-state PDU (LSP):** Used to distribute link-state information
- **Partial sequence number PDU (PSNP):** Used to acknowledge and request missing pieces of link-state information
- **Complete sequence number PDU (CSNP):** Used to describe the complete list of LSPs in the LSDB of a router

Example

OSI IS-IS PDUs (Cont.)

Cisco.com

PDU between peers:

- **Network PDU = datagram, packet**
- **Data-link PDU = frame**

IS-IS	Data-link header (OSI family 0xFEFE)	IS-IS header (first byte is 0x83)	IS-IS TLVs
ES-IS	Data-link header (OSI family 0xFEFE)	ES-IS header (first byte is 0x82)	ES-IS TLVs
CLNP	Data-link header (OSI family 0xFEFE)	CLNP header (first byte is 0x81)	CLNS

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 5-10

The OSI stack defines a unit of data as a PDU. OSI recognizes a frame as a data-link PDU and a packet (or datagram, in the IP environment) as a network PDU.

The figure shows three types of PDUs (IEEE 802.2 Logical Link Control [LLC] encapsulation). IS-IS and ES-IS PDUs are encapsulated directly in a data-link PDU, while true CLNP (data) packets contain a full CLNP header between the data-link header and any higher-layer CLNS information.

The IS-IS and ES-IS PDUs contain variable-length fields, depending on the function of the PDU. Each field contains a type code, a length, and the appropriate values. The fields of information are Type, Length, Value (TLV).

Link-State Packets

This topic describes how LSPs define the characteristics of a router.

Link-State Packets Representing Routers
Cisco.com

Router describes itself with the LSP.

- **LSP header contents:**
 - PDU type, length, LSP ID, sequence number, remaining lifetime
- **TLV variable-length fields:**
 - **IS neighbors**
 - **ES neighbors**
 - **Authentication information**
 -

The diagram illustrates the structure of an LSP. It starts with an **LSP Header**, which contains fields for PDU type, length, LSP ID, sequence number, and remaining lifetime. Following the header are one or more **TLV** (Type-Length-Value) variable-length fields. The first TLV is labeled **IS Neighbors**, the second **ES Neighbors**, and there is an ellipsis indicating additional fields.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-11

In IS-IS, characteristics of a router are defined by an LSP. The LSP of the router contains an LSP header and TLV fields.

- An LSP header describes the following:
 - The PDU type and length
 - The LSP ID and sequence number used to identify duplicate LSPs and to ensure that the latest LSP information is stored in the topology table
 - The remaining lifetime for the LSP, which is used to age out LSPs
- TLV variable-length fields contain the following:
 - The neighbor ISs of the router that are used to build the map of the network
 - The neighbor ESs of the router
 - Authentication information that is used to secure routing updates
 - Attached IP subnets (optional for Integrated IS-IS)

LSP Representing Routers: LSP Header

Cisco.com

LSPs are sequenced to prevent duplication of LSPs.

- Assists with synchronization
- Sequence numbers begin at 1

Sequence numbers are increased to indicate the newest LSP.

- LSPs in LSDB have a remaining lifetime
- Allows synchronization
- Decreasing timer

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-12

LSPs are given sequence numbers that allow receiving routers to do the following:

- Ensure that they use the latest LSPs in their route calculations
- Avoid the entering of duplicate LSPs in the topology tables

When a router reloads, the sequence number is set to 1. The router then receives its previous LSPs back from its neighbors. These LSPs have the last valid sequence number before the router reloaded. The router records this number and reissues its own LSPs with the next-highest sequence number.

Each LSP has a remaining lifetime that is used by the LSP aging process to ensure the removal of outdated and invalid LSPs from the topology table after a suitable time. This process is known as the count to zero operation; 1200 seconds is the default start value.

LSP TLV Examples

Cisco.com

TLV	Type Code	Length Field	Value Variable Length
Area Address	1	Area ID length + 1	Areas
Intermediate System Neighbors	2	Neighbor count +1	IS neighbors
IP Internal Reachability	128	Number of connected prefixes	Connected IP prefixes – 4B metric, 4B prefix, 4B mask
IP External Reachability	130	Number of redistributed prefixes	Redistributed IP prefixes – 4B metric, 4B prefix, 4B mask

- Each set of information, called a *tuple*, includes a type code, length field, and value.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-13

Each LSP includes specific information about networks and stations attached to a router. This information is found in multiple TLV fields that follow the common header of the LSP. TLV is sometimes also referred to as Code, Length, Value (CLV). The TLV structure is a flexible way to add data to the LSP and an easy mechanism for adding new data fields that may be required in the future.

The figure shows examples of TLVs.

You can find documentation on important TLVs in ISO 10589 and RFC 1195.

Link-State Packets: Network Representation

Cisco.com

- Generally, physical links can be placed in the following two groups:
 - Broadcast: Multiaccess subnetworks that support addressing of a group of attached systems (LANs)
 - Point-to-point links, multipoint links, dynamically established links
- Only the following two link-state representations are available in IS-IS:
 - Broadcast for LANs
 - Point-to-point for all other topologies

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-14

Network topologies can be divided into two general types as follows:

- **Point-to-point networks:** Point-to-point links that are either permanently established (leased line, permanent virtual circuit [PVC]) or dynamically established (ISDN, switched virtual circuit [SVC])
- **Broadcast networks:** Multipoint WAN links or LAN links such as Ethernet, Token Ring, or FDDI

IS-IS supports the following two media representations for its link states:

- Broadcast for LANs and multipoint WAN links
- Point-to-point for all other media

Note IS-IS has no concept of a nonbroadcast multiaccess (NBMA) network. It is recommended that you use point-to-point links, such as point-to-point subinterfaces, over NBMA networks such as ATM, Frame Relay, or X.25.

Topologies

This topic describes the two topology types that give a network designer different ways to handle adjacency over a link.

Implementing Network Types in NBMA

Cisco.com

- **When implementing IS-IS in NBMA (like Frame Relay or ATM):**
 - Broadcast mode assumes fully meshed connectivity
 - In broadcast mode, you must map CLNS and include broadcast keyword
 - Point-to-point mode highly recommended (subinterfaces)

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-15

Cisco IOS software automatically uses broadcast mode for LAN links and multipoint WAN links. It uses point-to-point topology for point-to-point links, such as point-to-point subinterfaces and dialer interfaces.

There is no specific support for NBMA networks in IS-IS. When implemented in broadcast mode, IOS software assumes that the NBMA environment features a full mesh of PVCs.

You should use the **broadcast** keyword when creating the static maps because broadcast mode uses multicast updates. Use a **broadcast** keyword when mapping the remote IP address to the local DLCI on a Frame Relay interface.

When you use multipoint WAN links like multipoint Frame Relay interfaces, you must also create static CLNS maps (in addition to the IP maps); for example, using the command **frame-relay map clns <dcli-number> broadcast**.

It is highly recommended that you implement NBMA environments, such as Frame Relay, as point-to-point links instead of multipoint links.

Broadcast Networks

This topic identifies the features of broadcast networks. Broadcast networks are LAN interfaces or multipoint WAN interfaces.

Note Broadcast mode is recommended for use only on LAN interfaces.

Broadcast Adjacency

Cisco.com

- **Used for LAN and multipoint WAN interfaces**
- **Adjacency recognized through hellos**
- **DIS is elected based on the following criteria:**
 - Only routers with adjacencies are eligible
 - Highest interface priority
 - Highest SNPA (MAC) breaks ties

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-16

You establish separate adjacencies for Level 1 and Level 2. If two neighboring routers in the same area run both Level 1 and Level 2, they establish two adjacencies, one for each level. The router stores the Level 1 and Level 2 adjacencies in separate Level 1 and Level 2 adjacency tables.

On LANs, routers establish the two adjacencies with specific Layer 1 and Layer 2 IIH PDUs. Routers on a LAN establish adjacencies with all other routers on the LAN (unlike OSPF, where routers establish adjacencies only with the designated router [DR]).

IIH PDUs announce the area ID. Separate IIH packets announce the Level 1 and Level 2 neighbors. Adjacencies form based on the area address communicated in the incoming IIH and the type of router (Level 1 or Level 2). Following is an example:

- Level 1 routers accept Level 1 IIH PDUs from their own area and establish adjacencies with other routers in their own area.
- Level 2 routers (or the Level 2 process within any Level 1-2 router) accept only Level 2 IIH PDUs and establish only Level 2 adjacencies.

Dijkstra's algorithm requires a virtual router (pseudonode), called the Designated Intermediate System (DIS) in order to build a directed graph for broadcast media. Criteria for DIS selection are, first, highest priority (the priority value is configurable) and, second, highest MAC address. The elected DIS then generates an LSP representing a virtual router connecting all attached routers to a star-shaped topology.

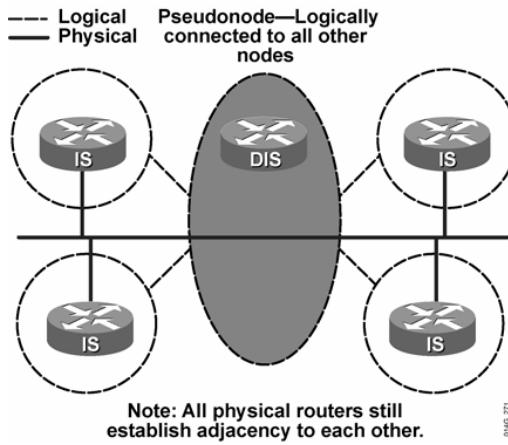
During the DIS election, a set of adjacent routers compare interface priority values. The router with the highest interface priority is the preferred selection with the SNPA address or MAC address, breaking any ties.

Cisco router interfaces have a default Level 1 and Level 2 priority of 64. You can configure the priority from 0 to 127 using the **isis priority** command. The Level 1 DIS and the Level 2 DIS on a LAN may or may not be the same router because an interface can have different Level 1 and Level 2 priorities.

A selected router is not guaranteed to remain the DIS. Any adjacent IS with a higher priority automatically takes over the DIS role. This behavior is called preemptive. Because the IS-IS LSDB is synchronized frequently on a LAN, giving priority to another IS over the DIS is not a significant issue. Unlike OSPF, IS-IS does not use a backup DIS, and routers on a LAN establish adjacencies both with all other routers and with the DIS.

LSP Representing Routers: LAN Representation

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-17

04UG_271

Rather than having each router connected to the LAN advertise an adjacency with every other router on the LAN, the entire network is considered a router, called the pseudonode. Each router just advertises a single adjacency to the pseudonode. Otherwise, each IS on a broadcast subnetwork with n connected ISs requires $(n)(n - 1) / 2$ adjacency advertisements. Generating LSPs for each adjacency creates considerable overhead in terms of LSDB synchronization.

When a pseudonode is being used, each IS is required to advertise only a single adjacency to the pseudonode. The pseudonode is represented by a DIS, which generates the pseudonode LSPs. A pseudonode LSP details only the adjacent ISs (for example, the ISs connected to that LAN). The pseudonode LSP is used to build the map of the network and to calculate the shortest path first (SPF) tree. The pseudonode LSP is the equivalent of a network LSA in OSPF.

In IS-IS, all routers on the LAN establish adjacencies with all other routers and with the DIS. Therefore, if the DIS fails, another router takes over immediately with little or no impact on the topology of the network. There is no backup DIS.

In OSPF, once the DR and backup designated router (BDR) are selected, the other routers on the LAN establish full adjacencies with the DR and BDR. In case of DR failure, the BDR is promoted to DR and a new BDR is elected.

Point-to-Point Networks

This topic describes the levels involved in point-to-point networks.

Level 1 and Level 2 LSPs and IIHs

Cisco.com

- Two-level nature of IS-IS requires separate types of LSPs: Level 1 and Level 2 LSPs
- LSPs sent as unicast on point-to-point
- LSPs sent as multicast on broadcast
- DIS is representative of LAN:
 - DIS sends pseudo-Level 1 and Level 2 LSPs for LAN
 - Separate DIS for Level 1 and Level 2; no backup DIS
- LAN uses separate Level 1 and Level 2 IIH
- Point-to-point uses a common IIH format

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-18

Level 1 and Level 2 LSP

IS-IS uses a two-level area hierarchy. The link-state information for these two levels is distributed separately, which results in Level 1 LSPs and Level 2 LSPs. Each IS originates its own LSPs (one for Level 1 and one for Level 2).

On a LAN, one router (the DIS) sends out LSP information on behalf of the LAN. The DIS creates a pseudonode, which is the representation of the LAN. The DIS sends out the separate Level 1 and Level 2 LSPs for the pseudonode. The Level 1 DIS and the Level 2 DIS on a LAN may or may not be the same router because an interface can have different Level 1 and Level 2 priorities.

LSPs on broadcast media (LANs) are sent as multicast, and LSPs on point-to-point links are sent as unicast.

Level 1 and Level 2 IIH

IIHs are used to establish and maintain neighbor adjacency between ISs.

On a LAN, separate Level 1 and Level 2 IIHs are sent periodically as multicasts. The default hello interval is every 10 seconds; however, the hello interval timer is adjustable. On a LAN, the hello packets are multicast to a multicast MAC address. Level 1 announcements are sent to the AllL1IS multicast MAC address 0180.C200.0014, and Level 2 announcements are sent to the AllL2IS multicast MAC address 0180.C200.0015. The default hello interval for the DIS is three times faster than the interval for the other routers so that DIS failures can be quickly detected. Unlike the DR and BDR in OSPF, there is no backup DIS in IS-IS.

A neighbor is declared dead if two hellos are not received within the hold time. Hold time is calculated as the product of the hello multiplier and hello time. The default hello time is 10 seconds and the default multiplier is three. Therefore, the default hold time is 30 seconds.

Unlike LAN interfaces with separate Level 1 and Level 2 IIH, point-to-point links have a common point-to-point IIH format that specifies whether the hello relates to Level 1 or Level 2 or both. Point-to-point hellos are sent to the unicast address of the connected router.

Link-State Database Synchronization

This topic compares broadcast and point-to-point links.

Comparing Broadcast and Point-to-Point Topologies		
	Broadcast	Point-to-Point
Usage	LAN, full-mesh WAN	PPP, HDLC, partial-mesh WAN
Hello Timer	3.3 sec for DIS, else 10 sec	10 sec
Adjacencies	$n(n - 1) / 2$	$n - 1$
Uses DIS	Yes	No
IIL Type	Level 1 IIL, Level 2 IIL	Point-to-point IIL

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-19

This figure summarizes the differences between broadcast and point-to-point links.

The Flooding Subprotocol

Cisco.com

- Single procedure for flooding, aging, and updating of LSPs.
- Level 1 LSPs are flooded within area.
- Level 2 LSPs are flooded throughout Level 2 subdomain.
- Large PDUs are divided into fragments that are independently flooded.
- Each PDU is assigned an LSP number, starting at 0 and incrementing by one.
- Separate LSDBs are maintained for Level 1 and Level 2 LSPs.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-20

An IS-IS update process is responsible for flooding the LSPs throughout the IS-IS domain. An LSP is typically flooded to all adjacent neighbors except the neighbor from which it was received. Level 1 LSPs are flooded within their local areas. Level 2 LSPs are flooded throughout the backbone.

Each IS originates its own LSP (one for Level 1 and one for Level 2). These LSPs are identified by the system ID of the originator and an LSP number starting at 0. If an LSP exceeds the maximum transmission unit (MTU), it is fragmented into several LSPs, numbered 1, 2, 3, and so on.

IS-IS maintains the Level 1 and Level 2 LSPs in separate LSDBs.

When an IS receives an LSP, it examines the checksum and discards any invalid LSPs, flooding them with an expired lifetime age. If the LSP is valid and newer than what is currently in the LSDB, it is retained, acknowledged, and given a lifetime of 1200 seconds.

The age is decremented every second until it reaches zero (0), at which point the LSP is considered to have expired. Once the LSP has expired, it is kept for an additional 60 seconds before it is flooded as an expired LSP.

LSDB Synchronization

Cisco.com

- **SNP packets are used to ensure synchronization and reliability.**
 - Contents are LSP descriptions
- **PSNP is used for the following:**
 - For acknowledgment of LSPs on point-to-point links
 - To request missing pieces of LSDB
- **CSNP is used for the following:**
 - Periodically by DIS on LAN to ensure reliability
 - On point-to-point link when the link comes up

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-21

Sequence number PDUs (SNPs) are used to acknowledge the receipt of LSPs and to maintain LSDB synchronization. There are two types of SNPs: complete SNP (CSNP) and partial SNP (PSNP). The use of SNPs differs between point-to-point and broadcast media.

CSNPs and PSNPs share the same format; that is, each carries summarized LSP information. The main difference is that CSNPs contain summaries of all LSPs in the LSDB, while PSNPs contain only a subset of LSP entries.

Separate CSNPs and PSNPs are used for Level 1 and Level 2 adjacencies.

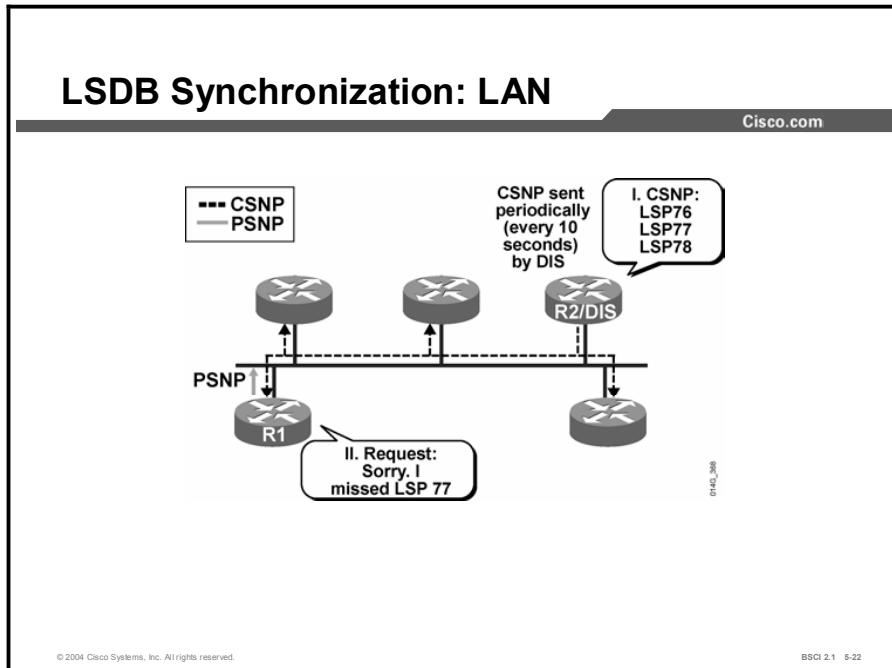
Adjacent IS-IS routers exchange CSNPs to compare their LSDB. In broadcast subnetworks, only the DIS transmits CSNPs. All adjacent neighbors compare the LSP summaries received in the CSNP with the contents of their local link-state databases to determine if their LSDBs are synchronized or have the same copies of LSPs as other routers for the appropriate levels and area of routing.

CSNPs are periodically multicast (every 10 seconds) by the DIS on a LAN to ensure LSDB accuracy.

If there are too many LSPs to include in one CSNP, the LSPs are sent in ranges. The CSNP header indicates the starting and ending LSP ID in the range. If all LSPs fit the CSNP, the range is set to default values.

Adjacent IS-IS routers use PSNPs to acknowledge the receipt of LSPs and to request transmission of missing or newer LSPs.

Example



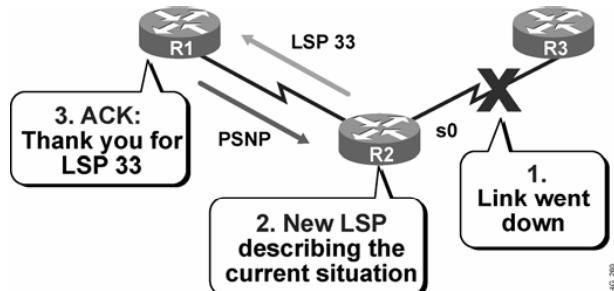
The DIS periodically (every 10 seconds) sends CSNPs that list the LSPs it holds in its LSDB. This update is a broadcast to all IS-IS routers on the LAN.

In the example, router 1 compares this list of LSPs with its topology table and realizes that it is missing one LSP. Therefore, it sends a PSNP to the DIS (router 2) to request the missing LSP.

The DIS reissues only that missing LSP (LSP 77), and router 1 acknowledges it with a PSNP (not shown).

LSDB Synchronization: Point-to-Point

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-23

In contrast to broadcast links such as LAN links, on point-to-point links, CSNPs are not periodically sent. A CSNP is sent only once, when the point-to-point link first becomes active. After that, LSPs are sent to describe topology changes, and they are acknowledged with a PSNP.

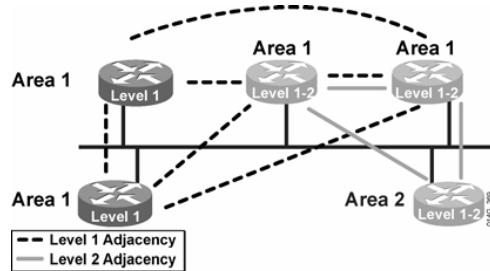
This figure shows what happens on a point-to-point link when a link failure is detected. The sequence is as follows:

1. A link fails.
2. Router 2 notices this failure and issues a new LSP noting the change.
3. Router 1 receives the LSP, stores it in its topology table, and sends a PSNP back to router 2 to acknowledge receipt of the LSP.

LAN Adjacencies

Cisco.com

Adjacencies are established based on the area address announced in the incoming IIHs and the type of the router.



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-24

IIH PDUs announce the area ID. On LANs, separate IIH packets announce the Level 1 and Level 2 neighbors.

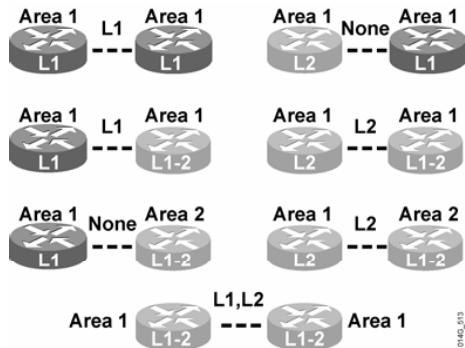
For example, where a LAN has routers from two areas attached, the following processes apply:

- The routers from one area accept Level 1 IIH PDUs only from their own area and therefore establish adjacencies only with their own area routers.
- The routers from a second area similarly accept Level 1 IIH PDUs only from their own area.

The Level 2 routers (or the Level 2 process within any Level 1-2 router) accept only Level 2 IIH PDUs and establish only Level 2 adjacencies.

WAN Adjacencies

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-26

On point-to-point links (that is, on a point-to-point WAN link), the IIH PDUs are common to both levels but announce the level type and the area ID in the hellos.

- Level 1 routers in the same area (which includes links between Level 1 and Level 1-2 routers) exchange IIH PDUs that specify Level 1 and establish a Level 1 adjacency.
- Level 2 routers (in the same area or between areas, and including links between Level 2 only and Level 1-2 routers) exchange IIH PDUs that specify Level 2 and establish a Level 2 adjacency.
- Two Level 1-2 routers in the same area establish both Level 1 and Level 2 adjacencies and maintain these with a common IIH PDU that specifies the Level 1 and Level 2 information.

Two Level 1 routers that are physically connected, but that are not in the same area, can exchange IIHs, but they do not establish adjacency because the area IDs do not match.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- The OSI address plan determines the IS-IS routing. Areas are identified and unique IDs are given to each device.
- PDUs encapsulate directly into an OSI data-link frame. Broadcast and nonbroadcast are the two main media types that represent physical links.
- IS-IS recognizes point-to-point and broadcast as the two topology types to handle adjacency over a link.
- Broadcast networks are LAN interfaces or multipoint WAN interfaces.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-26

Summary (Cont.)

Cisco.com

- IS-IS is a link-state protocol that permits partitioning of an IS-IS routing domain into areas.
- Adjacency forms based on the area address announced in the incoming IIH and the type of router.
- The update process floods LSPs throughout the domain.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-27

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 statements are part of OSI routing logic? (Choose two.)
- A) A Level 1-2 router should compare the destination area ID to its own area ID and, if they are the same, route at Level 1.
 - B) A Level 1-2 router should compare the destination area ID to its own area ID and, if they are different, route at Level 1.
 - C) A Level 1-2 router should compare the destination area ID to its own area ID and, if they are the same, route at Level 2.
 - D) A Level 1-2 router should compare the destination area ID to its own area ID and, if they are different, route at Level 2.
- Q2) Which two options complete the following statement? (Choose two.)
Adjacencies are formed in IS-IS between _____.
- A) ISs in the same area
 - B) pseudonodes
 - C) two ISs doing routing at the same level (Level 1 or Level 2)
 - D) interfaces on a broadcast network
- Q3) How are IS-IS PDUs transported?
- A) within IP packets
 - B) within CLNS packets
 - C) as 802.2 frames
 - D) reliably using TCP
- Q4) What are the four types of IS-IS PDUs? (Choose four.)
- A) hello
 - B) SNAP
 - C) LSP
 - D) PSNP
 - E) CSNP
 - F) IP/IPX
 - G) OSPF

- Q5) What does TLV stand for?
- A) Time, Level, Value
 - B) Text, Level, Volume
 - C) Time, Length, Volume
 - D) Type, Length, Value
- Q6) Which three topology types are supported by IS-IS? (Choose three.)
- A) broadcast for LAN links
 - B) broadcast for multipoint WAN links
 - C) stub for networks with a single exit
 - D) point-to-point for LAN links
 - E) point-to-point for point-to-point WAN links
 - F) NBMA for WAN links
- Q7) How does IS-IS deal with DIS failures?
- A) The Backup IS (BIS) asserts itself as the new DIS.
 - B) The failure is recognized quickly and a new DIS is elected. Since IS-IS synchronizes LSDBs frequently on a LAN, this is rarely a problem.
 - C) The network reverts to general topology, and every IS forms an adjacency with every other IS.
 - D) It does not. The DIS must be restored quickly to prevent communication problems.
- Q8) How does IS-IS adapt the directed graph approach (implicit in Dijkstra's algorithm) for use in a multipoint environment such as Ethernet?
- A) It uses a pseudonode.
 - B) It uses a system ID.
 - C) The algorithm is amended.
 - D) Dijkstra's algorithm is used only on point-to-point links.
- Q9) Which four technologies are appropriate for point-to-point topology? (Choose four.)
- A) ATM PVC
 - B) DS1
 - C) Ethernet
 - D) Frame Relay
 - E) Token Ring
 - F) ISDN Dial-on-Demand

- Q10) What is the function of CSNPs?
- A) to request a missing LSP
 - B) to acknowledge an LSP
 - C) to provide alerts
 - D) to maintain LSDB synchronization

Quiz Answer Key

Q1) A, D

Relates to: Intra-Area and Interarea Addressing and Routing

Q2) A, C

Relates to: IS-IS System Routing Levels

Q3) C

Relates to: IS-IS Protocol Data Units

Q4) A, C, D, E

Relates to: IS-IS Protocol Data Units

Q5) D

Relates to: Link-State Packets

Q6) A, B, E

Relates to: Topologies

Q7) B

Relates to: Broadcast Networks

Q8) A

Relates to: Broadcast Networks

Q9) A, B, D, F

Relates to: Point-to-Point Networks

Q10) D

Relates to: Link-State Database Synchronization

Basic Operations of Integrated IS-IS in an IP and CLNS Environment

Overview

This lesson discusses the mechanics of IS-IS operation in an IP and CLNS environment.

Relevance

When IS-IS is installed to support IP exclusively, network devices must also be configured to use the OSI CLNS protocol. Each IS-IS router requires a network entity title (NET), and IS-IS packets are directly encapsulated onto the data-link layer instead of traveling inside IP packets. You should understand OSI CLNS characteristics before you configure Integrated IS-IS.

Objectives

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

- Explain the purpose of Integrated IS-IS NET addressing for advertising IP networks
- Explain the path selection process for IS-IS routing
- Demonstrate how an IP forwarding database is constructed
- Use the output of **show** commands

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Integrated IS-IS NET Addressing**
- **Criteria and Path Selection for IS-IS Area Routing**
- **Building an IP Forwarding Database**
- **Using show Commands**
- **Summary**
- **Quiz**

Integrated IS-IS NET Addressing

A NET address identifies a device (an IS or ES) and not an interface. In this way, a NET address critically differs from an IP address. This topic describes supporting IS-IS for IP routing. Keep in mind that each router still requires a NET.

Integrated IS-IS: NET Address Planning

Cisco.com

- **Common CLNS parameters (NET) and area planning are still required even in an IP environment.**
- **Even when Integrated IS-IS is used for IP routing only, routers still establish CLNSadjacencies and use CLNS packets.**

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 5-4

Cisco Systems routers are able to use IS-IS for the following two purposes:

- CLNS support
- IP support (Integrated IS-IS) in addition to CLNS, or for IP only

Even if you use IP routing only over Integrated IS-IS, each IS-IS router must have a NET address configured because Integrated IS-IS depends on the support of CLNS routing.

- OSI protocols (hello PDUs) are used to form the neighbor relationship between routers.
- SPF calculations rely on a configured NET address to identify the routers.

When you are implementing IP addressing, you should do so at the interface, and each interface must belong to a different subnet. A NET address applies to the entire IS-IS router. For instance, each router has a unique NET address that identifies the entire router, not a particular interface.

Recall that the NET contains both the area address and the unique device address. These two portions of the address form the basis for IS-IS routing.

A device identifies other devices within its own area based on matching area addresses in their NET. It then knows that it can communicate with these other devices without using a default route. A default route is injected into the area by the Level 1-2 router. If the area addresses do not match, then the device knows that it must forward that traffic to its nearest Level 1-2 router.

When you are using IS-IS to route IP traffic, IP subnets are treated as leaf objects associated with IS-IS areas. When you use IP to transmit, the router looks up the destination network in its routing table. If the network belongs to a different area, then that traffic must also be forwarded to the nearest Level 1-2 router.

Scalability is achieved by minimizing the size of the LSDB and routing tables, the amount of processing, and the amount of network updates; in other words, by using route summarization wherever possible.

Route summarization can be accomplished only where the address planning permits grouping addresses together by a common prefix. This condition is true for OSI and IP. It is, therefore, very important to carefully plan the IS-IS areas, NET addresses, and IP addresses.

Criteria and Path Selection for IS-IS Area Routing

This topic describes how IS-IS adjacencies and path selection processes center on the OSI-based understanding of network topology.

OSI Area Routing: Building an OSI Forwarding Table

Cisco.com

- When databases are synchronized, Dijkstra's algorithm (SPF) is run on the LSDB to calculate the SPF tree.
 - Criteria: The shortest path to the destination is the lowest total sum of metrics.
 - Separate route calculations are made for Level 1 and Level 2 areas in Level 1-2 routers.
- PRC is run to calculate ES reachability.
- Best paths are placed in the OSI Level 1 and Level 2 forwarding tables.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-5

IS-IS uses an OSI forwarding database (routing table) to select the best path to a destination. To build the OSI forwarding database, the CLNS routing table, routers use the following process:

- Use the LSDB to calculate the SPF tree to OSI destinations, NETs. The total of the link metrics along each path determines the shortest path to any given destination.
- Understand that Level 1 and Level 2 routes have separate LSDBs; therefore, routers run SPF twice, once for each level, and create separate SPF trees for each level.
- Calculate ES reachability with a partial route calculation (PRC) based on the Level 1 and Level 2 SPF trees. There are no OSI ESs in a pure IP Integrated IS-IS environment.
- Insert the best paths in the CLNS routing table (OSI forwarding database).

Building an IP Forwarding Database

The processes and outputs for the OSI part of the IS-IS process are the same for pure OSI IS-IS routing. This topic demonstrates how an IP forwarding database is constructed.

Building an IP Forwarding Table

Cisco.com

PRC is also run to calculate IP reachability.

- Since IP and ES are represented as leaf objects, they do not participate in SPF.

Best paths are placed in the IP forwarding table following IP preferential rules.

- They appear as Level 1 or Level 2 IP routes.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

Integrated IS-IS includes IP information in the LSPs, treating it as if it were ES information. For IS-IS, IP is information regarding the leaf connections to the SPF tree. Therefore, updating IP reachability requires only a PRC, similar to ES reachability.

The PRC generates best-path choices for IP routes and offers the routes to the routing table, where they are accepted based on normal IP routing table rules. For example, if there is more than one routing protocol running, then the router compares administrative distance. When the IP IS-IS routes are entered in the routing table, they are shown as via Level 1 or Level 2, as appropriate.

The separation of IP reachability from the core IS-IS network architecture provides Integrated IS-IS better scalability than, for example, OSPF, as follows:

- OSPF sends LSAs for individual IP subnets. If an IP subnet fails, then the LSA floods through the network. In all circumstances, all routers must run a full SPF calculation, which is extremely CPU-intensive.
- Integrated IS-IS builds the SPF tree from CLNS information. If an IP subnet fails in an Integrated IS-IS, the LSP floods through the network, which is the same for OSPF. If this is a leaf (stub) IP subnet (that is, if the loss of the subnet does not affect the underlying CLNS architecture), the SPF tree is unaffected; therefore, only a PRC occurs.

Example

Cisco.com

```
The IP addresses on loopbacks of routers are 1.0.0.1/8-R1,
2.0.0.1/8-R2, 4.0.0.1/8-R4 and 5.0.0.1/8-R5.
R2#sh ip route
i L1 1.0.0.0/8 [115/10] via 10.12.0.1, Ser0 - (R1)
i L1 4.0.0.0/8 [115/10] via 10.24.0.4, Ser1 - (R4)
i L2 5.0.0.0/8 [115/10] via 11.0.0.10, Eth0 - (R5)
```

0102_202

The diagram illustrates a network topology with three routers: R1, R2, and R5. Router R1 is located in a cloud labeled 'R1 - L1' and has a loopback interface L1. Router R2 is also in a cloud labeled 'R2 - L1L2' and has a serial interface S0 connected to R1's L1 and a loopback interface L1. Router R5 is in a cloud labeled 'R5 - L2' and is connected to R2 via an Ethernet interface E0. Router R2's L1 interface is also connected to R4, which is in a cloud labeled 'R4 - L1'. The connections are shown with arrows indicating the direction of traffic flow.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-7

In the figure, the **show ip route** command has been given to display the IP IS-IS routes in the IP routing table. The table shows routes to loopback interfaces on each router. The “i” indicates that the route sources are from IS-IS.

The “L1” and “L2” show whether the IS-IS path to these destination IP networks is via IS-IS Level 1 or Level 2 routing. The next-hop IP addresses are matched from the corresponding next-hop IS-IS neighbor routers.

For example, network 1.0.0.0 (the loopback interface on router 1) is considered a leaf node attached to router 1. For router 2 to reach network 1.0.0.0, router 2 computes the shortest path to reach the system ID of router 1 based on the IS-IS LSDB.

Because router 1 and router 2 are in the same area, routing between router 1 and router 2 is based on system ID. In this case, the best path for router 2 to reach the system ID of router 1 is via the serial 0 interface that directly connects to router 1.

Using show Commands

This topic discusses using the output of **show** commands to help in verifying and troubleshooting CLNS IS-IS structures.

Troubleshooting Commands: CLNS

Cisco.com

Router#	show clns
	• Displays information about the CLNS network
Router#	show clns protocol [tag]
	• Lists the protocol-specific information
Router#	show clns interface [type number]
	• Lists the CLNS-specific information about each interface
Router#	show clns neighbors [type number] [detail]
	• Displays both ES and IS neighbors

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-8

You can use the following **show clns** commands to verify the router configuration and to troubleshoot the Integrated IS-IS network:

- **show clns:** This command displays general information about the CLNS network.
- **show clns protocol:** This command displays information for the specific IS-IS processes in the router.
- **show clns interface:** This command displays information about the interfaces that currently run IS-IS.
- **show clns neighbors:** This command displays IS and ES neighbors, if there are any. The neighbors are the routers with which this router has IS-IS adjacencies. The optional keyword **detail** displays comprehensive information about the neighbors. If **detail** is not specified, the neighbors are listed without any details. You can reduce the list of those neighbors across a particular interface if you specify the interface in the command.

Troubleshooting Commands: CLNS and IS-IS

Cisco.com

Router#

show isis route

- Displays IS-IS Level 1 routing table
(requires that CLNS routing be enabled)

Router#

show clns route

- Displays CLNS routing table

Router#

show isis database

- Displays the IS-IS LSDB

Router#

show isis topology

- Displays IS-IS least-cost paths to destinations

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-9

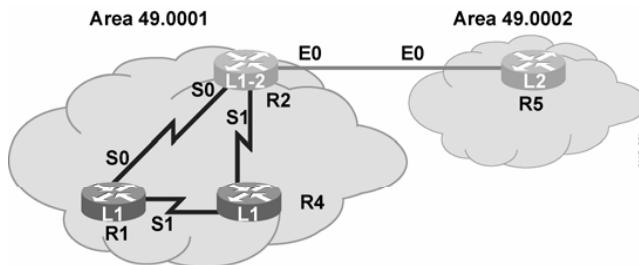
You can use the following **show** commands to verify the router configuration and to troubleshoot the Integrated IS-IS network:

- **show isis route:** This command displays the IS-IS Level 1 routing table, which includes all other system IDs in the area. This command is available only if CLNS routing is enabled both globally and at the interface level.
- **show clns route:** This command displays the IS-IS Level 2 routing table.
- **show isis database:** This command displays the contents of the IS-IS LSDB. To force IS-IS to refresh its LSDB and recalculate all routes, issue the **clear isis** command, specifying the IS-IS process tag or using an asterisk (*) to clear all IS-IS processes.
- **show isis topology:** This command displays the Level 1 and Level 2 topology tables, which show the least-cost IS-IS paths to the ISs.

OSI Intra-Area and Interarea Routing

Cisco.com

Routing in a Two-Level Area Structure



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-10

This figure shows four routers in two areas. Routers 1, 2, and 4 belong to area 49.0001. Router 5 belongs to area 49.0002. Routers 1 and 4 are Level 1 routers doing only Level 1 routing. Router 2 is a Level 1-2 router doing both Level 1 and Level 2 routing. Router 5 is a Level 2 router doing only Level 2 routing.

This figure forms the basis for the following **show** command examples.

Level 1 and Level 2 Topology Table

Cisco.com

```
R1# show isis topology

IS-IS paths to level-1 routers
System Id      Metric  Next-Hop    Interface  SNPA
R1              --      R2          Se0        *HDLC*
R2              10      R4          Se1        *HDLC*
R4              10      R4          Se1        *HDLC*

R2# show isis topology

IS-IS paths to level-1 routers
System Id      Metric  Next-Hop    Interface  SNPA
R1              10      R1          Se0        *HDLC*
R2              --
R4              10      R4          Se1        *HDLC*
IS-IS paths to level-2 routers
System Id      Metric  Next-Hop    Interface  SNPA
R2              --
R5              10      R5          Et0       0010.7bb5.9e20
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-11

The **show isis topology** command displays the topology databases with the least-cost paths to destination ISs.

Notice that the output for router 1 (a Level 1 router) shows the topology database for Level 1 only and the output for router 2 (a Level 1-2 router) shows that separate topology databases exist for Level 1 and Level 2.

The fields in the topology database are common for both levels of routing. They are as follows:

- The system ID shows the NET of the destination IS. Cisco IOS software uses dynamic host-name mapping (RFC 2763) to map the system ID to a host name that is available to the router.
- The metric displays the sum of the metrics on the least-cost path to the destination.
- The next-hop column displays the next IS along the path to a destination.
- The interface column shows the output interface that leads to the system listed in the next-hop column.
- The SNPA column contains the OSI Layer 2 address of the next hop. HDLC is shown as the SNPA across an HDLC serial interface. The SNPA across an Ethernet interface will be the system ID (MAC address). The SNPA can also be the DLCI if it is across a Frame Relay interface.

The topology database on router 1 (a Level 1 router) shows only routers within the local area. Router 1 is doing only Level 1 routing, and thus does not know of any routers outside its area. Traffic bound for other areas would be forwarded to the nearest router doing Level 2 routing, in this case, router 2.

Router 2 is doing both levels of routing. It thus maintains two topology databases. The Level 1 database looks very much like the router 1 database; only routers within the local area are listed. The Level 2 database is where the external router, router 5, finally shows up.

Intra-Area Routing on Router 1

Cisco.com

```
R1# show clns route

CLNS Prefix Routing Table
49.0001.0000.0000.0001.00, Local NET Entry

R1# show isis route

IS-IS Level-1 Routing Table - version 312
System Id Next-Hop Interface SNPA Metric State
R2          R2      Se0     *HDLC*  10    Up    L2-IS
R4          R4      Se1     *HDLC*  10    Up
R1          --
Default route out of area - (via 1 L2-attached IS)
System Id Next-Hop Interface SNPA Metric State
R2          Se0     *HDLC*  10    Up
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-12

The **show clns route** command on router 1 displays the CLNS destinations to which this router routes packets. Router 1 displays only its local NET entry because it is a Level 1-only router; therefore, router 1 has no Level 2 area routes to display.

The **show isis route** command on router 1 shows the Level 1 routes to IS-IS neighbors. Router 1 is aware of the other Level 1 routers in its area.

The Level 1-2 router (router 2) appears in the Level 1 routing table by virtue of its Level 1 connection, with a note at the end of the entry to show that it also acts as a Level 2 router. The closest Level 1-2 router also appears as the default route out of the area.

The next-hop IS, the interface over which the next hop is reached, the SNPA, and the summed metric to that destination for all IS routes are shown. The neighbors show that their state is up to indicate that the hello process has successfully established an adjacency.

Intra-Area and Interarea Routing on Router 2

Cisco.com

```
R2# show clns route

CLNS Prefix Routing Table
49.0001.0000.0000.0002.00, Local NET Entry
49.0002 [110/10]
  via R5, IS-IS, Up, Ethernet0
49.0001 [110/0]
  via R2, IS-IS, Up

R2# show isis route

IS-IS Level-1 Routing Table - version 47
System Id  Next-Hop  Interface  SNPA   Metric  State
R4          R4        S0/1      *HDLC*  10      Up
R1          R1        S0/0      *HDLC*  10      Up
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-13

The same **show clns route** and **show isis route** commands executed on router 2 (the Level 1-2 router) present the following results:

- **show clns route:** This command displays the CLNS prefix routing table and the local NET entry. It displays the Level 2 routes to its own and neighbor areas. The “[110/10]” entry next to the area ID represents the administrative distance of IS-IS for CLNS, which is 110, and the IS-IS metric.

Note The administrative distance of IS-IS for IP is 115.

- **show isis route:** This command displays the Level 1 IS-IS routing table. Notice that there is no default route listed.

Note From the **show clns route** output, you can see that router 2 regards the route to its own area (49.0001) as being through itself, further emphasizing that the Level 1 and Level 2 processes operate separately.

Comparing the router 1 and router 2 outputs, notice that router 2, as a Level 2 IS, has a prefix table that contains routes outside the local area and that router 1 (a Level 1 router) has a default route. Also notice that each router acting as a Level 1 IS has all area neighbors in its IS-IS route table.

Simple Troubleshooting: What About CLNS Protocol?

Cisco.com

```
R2# show clns protocol
IS-IS Router: <Null Tag>
System Id: 1921.6800.1006.00  IS-Type: level-1-2
Manual area address(es):
 49.0001
Routing for area address(es):
 49.0001
Interfaces supported by IS-IS:
  Serial0 - IP
  Ethernet0 - IP
Redistribute:
  static (on by default)
Distance for L2 CLNS routes: 110
RRR level: level-1
Generate narrow metrics: level-1-2
Accept narrow metrics: level-1-2
Generate wide metrics: none
Accept wide metrics: none
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-14

In the figure, the example output from the **show clns protocol** command shows the following:

- The integrated IS-IS process, its tag, if present, and the level types on the router
- The system ID and area ID for this router
- The interfaces using integrated IS-IS for routing, including whether they are routing for IP, CLNS, or both
- Any redistribution of other route sources
- Information about the distances for Level 2 CLNS routes and the acceptance and generation of metrics

Are Adjacencies Established?

Cisco.com

```
R2# show clns neighbors
SYSTEM ID      INTERFACE SNPA          STATE HOLDTIME  TYPE  PROTOCOL
R1             Se0      *HDLC*           Up    28          L1   IS-IS
R5             Et0      0000.0c92.de4c  Up    20          L2   IS-IS

R2# show clns interface serial 0
serial0 is up, line protocol is up
  Checksums enabled, MTU 1500, Encapsulation HDLC
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
  Congestion Experienced bit set at 4 packets
  CLNS fast switching disabled
  CLNS SSE switching disabled
  DBC compatibility mode OFF for this interface
  Next ESH/ISH in 12 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1
    Interface number 0x1, local circuit ID 0x101
    Level-1 Metric: 10, Priority: 64, Circuit ID: R2.00
    Number of active level-1 adjacencies: 1
    Next IS-IS Hello in 5 seconds
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 5-15

In the figure, the example output from the **show clns neighbors** command shows the following:

- The IS-IS neighbors
- The SNPAs and state
- The hold time, which is the timeout for receipt of no hellos, after which the neighbor is declared down
- The neighbor level and type

Also in this figure, the example of output from the **show clns interface** command shows the following:

- The interface runs IS-IS and attempts to establish Level 1 adjacencies.
- The interface numbers and circuit ID for IS-IS purposes.
- The metric or metrics for the interface.
- The priority for Designated Intermediate System (DIS) negotiation. Priority is not relevant in this case because it is a serial HDLC interface.
- The information regarding hello timers and the number of established adjacencies.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- NET addresses identify a device, and IP addresses identify an interface; each router requires a NET address.
- OSI forwarding databases, or the CLNS routing tables, are built by adhering to specific guidelines.
- System IDs of the destination OSI NSAP addresses determine the routing inside a Level 1 area.
- IS-IS databases are built on the CLNS table structure to allow routing outside the local link.
- Separating IP reachability from the core IS-IS network architecture provides Integrated IS-IS better scalability than OSPF.
- The show commands are used to troubleshoot CLNS IS-IS structures and Integrated IS-IS networks.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-16

References

For additional information, refer to these resources:

- RFC 995, *End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8437*.
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.
- Martey, A. *IS-IS Network Design Solutions*. Indianapolis, Indiana: Cisco Press; 2002.

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 function of the network entity title in IP networks?
- A) identify a router interface
 - B) identify a router process
 - C) identify a router
 - D) identify a subnet
- Q2) When does Dijkstra's algorithm run to determine the best path?
- A) after the PRC process is completed
 - B) when maximum age is reached
 - C) after databases are synchronized
 - D) at IS-IS startup
- Q3) What criteria does a router running Integrated IS-IS use to determine which routes to place in the routing (forwarding) table? (Choose two.)
- A) area addresses
 - B) administrative distance
 - C) information from a PRC
 - D) Level 2 routes only
- Q4) Which command displays the IS-IS Level 1 routing table?
- A) **show clns route**
 - B) **show ip neighbor**
 - C) **show isis route**
 - D) **which-route**
 - E) **show clns neighbor**
- Q5) Which command provides a list of all IS-IS areas?
- A) **show clns route**
 - B) **show ip route**
 - C) **which-route**
 - D) **show isis route**

- Q6) A Level 1-2 IS with the NET 49.000A.0000.0C12.3456.00 receives traffic going to 49.001A.0000.0C78.9AB.00. Which table does it use to route the traffic?
- A) IS-IS topology
 - B) Level 1 routing table
 - C) Level 2 routing table
 - D) CLNS routing table
- Q7) Which command reveals the redistribution processes in IS-IS?
- A) **show clns protocol**
 - B) **show clns interface**
 - C) **show isis route**
 - D) **show isis database**
- Q8) Which command would you use to view the router interfaces that are participating in IS-IS?
- A) **show clns protocol**
 - B) **show clns interface**
 - C) **show isis route**
 - D) **show isis database**

Quiz Answer Key

- Q1) C
Relates to: Integrated IS-IS NET Addressing
- Q2) C
Relates to: Criteria and Path Selection for IS-IS Area Routing
- Q3) B, C
Relates to: Building an IP Forwarding Database
- Q4) C
Relates to: Integrated IS-IS Tables
- Q5) B
Relates to: Using show Commands
- Q6) C
Relates to: Using show Commands
- Q7) A
Relates to: Using show Commands
- Q8) B
Relates to: Using show Commands

Configuring Basic Integrated IS-IS

Overview

This lesson explains basic IS-IS configuration.

Relevance

This lesson outlines specific commands necessary to implement IS-IS on a Cisco router. The commands for IS-IS are slightly different from those of the other IP routing protocols you have studied, so it is important to understand how to enable IS-IS processes. Additionally, the default settings for IS-IS can result in the inefficient use of router and network resources and suboptimal routing. Therefore, a network administrator also needs to know how to effectively tune IS-IS for optimum performance.

Objectives

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

- Describe the configuration process for Integrated IS-IS in an IP environment
- Configure IS-IS routing with default settings
- Optimize IS-IS by adjusting the IS type, circuit type, and metric
- Configure route summarization within IS-IS
- Use the output of **show** commands for verifying the IS-IS configuration and for troubleshooting IS-IS operations

Learner Skills and Knowledge

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

- CCNA certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Integrated IS-IS Configuration Steps**
- **Basic IS-IS Configuration Commands**
- **Optimizing IS-IS**
- **Scalable IS-IS in Large Networks**
- **Verifying IS-IS Configuration and Troubleshooting IS-IS Operations**
- **Summary**
- **Quiz**

Integrated IS-IS Configuration Steps

Four steps are required for the basic setup of IS-IS. Additional commands are available for fine-tuning the configuration.

Integrated IS-IS Configuration Steps

Cisco.com

Step 1: Define areas, prepare addressing plan (NETs) for routers, and determine interfaces.

Step 2: Enable IS-IS on the router.

Step 3: Configure the NET.

Step 4: Enable Integrated IS-IS on the proper interfaces. Do not forget interfaces to stub IP networks, such as loopbacks (although there are no CLNS neighbors there).

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-4

Before you configure Integrated IS-IS, you must map out the areas and plan the addressing. After that is done, you need three commands to enable Integrated IS-IS on a router for IP routing. You can then use additional commands to fine-tune the IS-IS processes.

The table describes the three basic commands used to enable Integrated IS-IS.

Command	Description
router isis	Enables IS-IS as an IP routing protocol and assigns a tag to the process (optional). Given at the global configuration mode.
net [number]	Identifies the router for IS-IS by assigning a NET to the router. Given at the router configuration mode.
ip router isis	Enables IS-IS on the interfaces that run IS-IS. (This approach is slightly different from most other IP routing protocols, where the interfaces are defined by network statements; there is no network statement under the IS-IS process.) Given at the interface configuration mode.

Step 1: Define Area and Addressing

Cisco.com

- **Area determined by NET prefix:**
 - Assign to support two-level hierarchy.
- **Addressing:**
 - **IP:** Plan to support summarization.
 - **CLNS:** Prefix to denote area. System ID must be unique.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-8

Recall that all intra-area traffic in IS-IS must traverse the Level 2 backbone area. Thus, CLNS addresses must be planned to execute a two-level hierarchy.

You must decide which routers will be backbone (Level 2) routers, which routers will be the Level 1-2 ABRs, and which will be internal area (Level 1) routers. If some routers must do both Level 1 and Level 2 routing, then the specific interfaces that will participate in each type of routing should be identified.

Remember that the CLNS address of a router is called the NET, and it consists of three main parts:

- The prefix, which identifies the area that the router is a part of
- The system ID, which uniquely identifies each device
- The network service access point (NSAP) selector (NSEL), which must be zero (0)

It is not enough to plan the IS-IS area addressing. You must also plan IP addressing to have a scalable network, and the IP addresses must be planned to allow for summarization of addresses.

Route summarization is the key idea that enables all the benefits of the hierarchical addressing design. Route summarization minimizes routing update traffic and resource utilization.

Be particularly careful when you configure the IP addressing on the router, because it is more difficult to troubleshoot IP address misconfigurations with IS-IS. The IS-IS neighbor relationships are established over OSI CLNS, not over IP. Because of this approach, two ends of a CLNS adjacency can have IP addresses on different subnets, with no impact to the operation of IS-IS.

Basic IS-IS Configuration Commands

This topic describes the commands used to configure Integrated IS-IS with the default settings.

Step 2: Enable IS-IS on the Router

Cisco.com

```
router(config)#
```

```
router isis [tag]
```

- **Enable the IS-IS routing protocol**
 - **tag**—name for a process
- **When routing of CLNS packets is also needed, use the clns routing command**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-6

The **router is-is** global configuration command enables Integrated IS-IS on the router. Optionally, you can apply a tag to identify multiple IS-IS processes. Just as multiple OSPF processes can be present on the same router, multiple IS-IS processes are possible.

The process name is significant only to the local router. If it is omitted, the Cisco IOS software assumes a tag of 0. If more than one IS-IS process is used, then the network plan should indicate which interfaces would participate in which IS-IS process.

CLNS routing is disabled by default. To enable CLNS routing in addition to IP routing, use the **clns routing** global configuration command. Additionally, you must enable CLNS routing at each interface.

Note

By default, the Cisco IOS software makes the router a Level 1-2 router.

Step 3: Configure the NET

Cisco.com

```
Router(config-router)#  
net network-entity-title
```

- **Configure an IS-IS NET address for the routing process**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-7

After the IS-IS process is enabled, the router must be identified for IS-IS by assigning a NET to the router with the **net** command given in router configuration mode.

Even when you use IS-IS for IP routing only (no CLNS routing enabled) you must still configure a NET. The NET is a combination of area number, a unique system identification number for each particular router, and the NSEL of 00 at the end.

The area number must be at least 1 byte in length and can be as long as 13 bytes. The system ID has a fixed length of 6 bytes in Cisco routers. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

Step 4: Enable Integrated IS-IS

Cisco.com

```
router(config-if)#  
ip router isis [tag]  
clns router isis [tag]
```

- Includes an interface in an IS-IS routing process

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-8

The final step is to select which interfaces participate in IS-IS routing. Interfaces that use IS-IS to distribute their IP information (and thus can also be used to establish IS-IS adjacencies) must be configured using the **ip router isis** interface command.

If there is more than one IS-IS process, interfaces must state the IS-IS process to which they belong by specifying the appropriate process name in the optional tag field. If no tag is listed, the IOS software assumes a tag value of 0. If there is only one IS-IS process active on the router, no tag value is needed.

Use the **clns router isis** interface command to enable the IS-IS routing process on an interface to support CLNS routing.

Example

IS-IS Configuration Steps: Simple Integrated IS-IS Example

Cisco.com

The configured router acts as an IP-only Level 1-2 router.

```
router isis
  net 49.0001.0000.0000.0002.00
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip router isis
!
interface serial 0
  ip address 10.1.2.1 255.255.255.0
  ip router isis
```

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 5-9

The figure shows an example of a simple Integrated IS-IS configuration for IP routing only; CLNS routing is not enabled. It specifies only one IS-IS process, thus the optional tag is not used.

The NET configures the router to be in area 49.0001 and assigns a system ID of 0000.0000.0002. IS-IS has been enabled on the Ethernet 0 and serial 0 interfaces.

Because no level has been configured under the IS-IS routing process, this router acts as a Level 1-2 router by default.

Optimizing IS-IS

Optimizing IS-IS facilitates its smooth functioning and maximizes its efficiency. This topic lists three commands that will help to optimize IS-IS operation.

Change IS-IS Router Level

Cisco.com

```
Router(config-router)#
  is-type {level-1 | level-1-2 | level-2-only}
```

- Configure the IS-IS level globally on a router; the default is Level 1-2.

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 5-10

Remember that the default configuration of IS-IS leaves the router with an IS type of Level 1-2. Although this configuration has the advantage of allowing all routers to learn of each other and pass routes without too much administrative oversight, it is not the most efficient way to build an IS-IS network.

Routers with the default configuration send out both Level 1 and Level 2 hellos and maintain both Level 1 and Level 2 LSDBs. Each router should be configured to support the minimum level of routing required, for the following reasons:

- Saves memory. If a router does not need the LSDB for one of the levels, it will not maintain one.
- Saves bandwidth. Hellos and LSPs will be sent only for the necessary level.

If a router is to operate only as an internal area router or a backbone router, then specify this configuration by entering the **is-type** router configuration command. To specify that the router act as an internal area (or Level 1)-only router, use the **is-type level-1** command.

To specify that the router act as a backbone (or Level 2)-only router, use the **is-type level-2-only** command. If the level type has been changed from the default, and the router needs to return to acting as a Level 1-2 router, then use the **is-type level-1-2** command.

Change IS-IS Interface Level

Cisco.com

```
Router(config-if)#  
isis circuit-type {level-1 | level-1-2 | level-2-only}
```

- **Configure the type of adjacency on an interface; the default is Level 1-2.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-11

Although the router can be a Level 1-2 router, it may not be required to establish both types of adjacencies over all interfaces. If a Level 1 router is connected to a particular interface, there is no need for it to send Level 2 hellos out that interface.

Similarly, if only a Level 2 router is connected to an interface, there is no need to send Level 1 hellos out that interface. It wastes bandwidth and router resources to try to establish adjacencies that do not exist.

To make IS-IS more efficient in these types of situations, configure the interface to send only the needed type of hellos. Perform this configuration by using the interface command **isis circuit-type** and specifying either the **level-1** or **level-2-only** keywords.

If the circuit type is not configured by default, Cisco IOS software attempts to establish both types of adjacencies over the interface (Level-1-2).

Change IS-IS Metric

Cisco.com

```
Router(config-if)#  
isis metric metric {level-1 | level-2}
```

- **Configure the metric for an interface; the default is 10.**
- **Metric value is from 1 - 63.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-12

Unlike most other IP protocols, IS-IS takes no account of line speed or bandwidth when it sets its link metrics. All interfaces are assigned a metric value of 10. In a network with links of varying types and speeds, this assignment can result in suboptimal routing.

To change the metric value, use the **isis metric metric {level-1 | level-2}** interface command. The metric can have different values for Level 1 and Level 2 over the same interface.

Example

Tuning IS-IS Configuration

Cisco.com

Area 49.0001

Area 49.0002

- **Change router type on router 1, router 4, and router 5**
- **Change interface levels on router 2**

```
hostname r1
router isis
net 49.0001.0000.0000.0001.00
is-type level-1
int s0
 ip router isis
 isis metric 35 level-1
int s1
 ip router isis
 isis metric 35 level-1
```

```
hostname r2
router isis
net 49.0001.0000.0000.0002.00
int e0
 ip router isis
isis circuit-type level-2-only
int s0
 ip router isis
isis circuit-type level-1
isis metric 35 level-1
int s1
 ip router isis
isis circuit-type level-1
isis metric 35 level-1
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-13

In the figure, there are two different areas. Area 49.0002 contains only one router (router 5) and needs to do only Level 2 routing. It is appropriate to change the IS type of router 5 to Level 2 only.

Area 49.0001 has three routers. Router 1 and router 4 are strictly internal area routers; they do not connect to routers in any other area. It is appropriate to configure these routers as IS type Level 1. Router 2 connects to the internal area routers and also to router 5, in a different area.

Router 2 must do both Level 1 and Level 2 routing, so it is left at the default setting. However, there is no need for router 2 to send Level 2 hellos out the interfaces connected to router 1 and router 4. It is appropriate to set the IS-IS circuit type of the serial 0 and serial 1 interfaces of router 2 to Level 1. Similarly, because the Ethernet 0 interface of router 2 connects only to a Level 2 router, you should set the IS-IS circuit type to Level 2 only.

Remember that the IS-IS metric for all interfaces is 10. In the topology shown, the serial links are slower than the Ethernet link. Additionally, it is possible that the serial links themselves all have different bandwidths.

Using the default metric does not give the routers a true picture of the value of each link, so the routers cannot make truly informed routing decisions. As shown in the sample configuration, you should change the IS-IS metric at each interface to reflect your preference for a link.

Scalable IS-IS in Large Networks

Routing protocol scalability is a function of the appropriate use of route summarization. This topic describes how to configure summarization within IS-IS.

IP Summarization

Cisco.com

```
Router(config-router)#  
summary-address prefix mask [level-1 | level-2 | level-1-2]
```

- **Creates summary**
- **Default is Level 2**

Example:

```
P3R1(config-router)# summary-address 10.3.2.0 255.255.254.0 level-2
```

- **Summarizes 10.3.2.0/23 into Level 2**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-14

An IS can be configured to aggregate a range of IP addresses into a summary address. The router summarizes IP routes into Level 1, Level 2, or both. The benefits of summarization include the following:

- Reduced routing table size
- Reduced LSP traffic and protection from flapping routes
- Reduced memory requirements
- Reduced CPU usage

Remove route summarization with the **no** form of the command.

Verifying IS-IS Configuration and Troubleshooting IS-IS Operations

To verify the IS-IS configuration and IP functionality of the Integrated IS-IS network, use the following commands (these commands can also be useful for troubleshooting problems with the IS-IS network):

- **show ip protocols:** Displays the active IP routing protocols, the interfaces on which they are active, and the networks for which they are routing.
- **show ip route:** Displays the IP routing table. The detail for a particular route or a list of all routes in the routing table from a particular process can be specified.

Example: Is Integrated IS-IS Running?

Cisco.com

```
Router# show ip protocols
```

```
R2# show ip protocols

Routing Protocol is "isis"
  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: isis
  Address Summarization:
    None
  Routing for Networks:
    Serial0
    Ethernet0
  Routing Information Sources:
    Gateway          Distance      Last Update
    11.0.0.1          115          00:11:44
    13.0.0.1          115          00:11:44
    14.0.0.1          115          00:11:44
  Distance: (default is 115)
```

- Displays the parameters and current state of the active routing protocol processes

This sample output from the **show ip protocols** command shows information about IP routing being done over Integrated IS-IS. In this example, IS-IS is running, it is not redistributing any other protocols, and address summarization has not been configured.

The example also shows that interfaces serial 0 and Ethernet 0 are taking part in Integrated IS-IS, that there are three sources of routing information (the neighboring routers), and that the administrative distance of Integrated IS-IS is 115.

Example: Are There Any IP Routes?

Cisco.com

router#

```
show ip route [address [mask]] | [protocol [process-id]]
```

```
R2#show ip route isis
```

```
i L1 11.0.0.0/8 [115/10] via 192.168.20.1, Serial0
i L1 13.0.0.0/8 [115/10] via 192.168.220.3, Ethernet0
i L1 14.0.0.0/8 [115/20] via 192.168.220.3, Ethernet0
```

- Displays the current state of the routing table

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 5-16

This sample output from the **show ip route isis** command shows only the IS-IS routes. These routes are all from Level 1, as indicated by the **i L1** tag.

Integrated IS-IS uses, by default, an administrative distance of 115. The metric shown for each route is taken from the IS-IS cost to the destination.

In the figure, for the value of [115/20], 115 is the Integrated IS-IS administrative distance and 20 is the IS-IS metric.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Four steps for the basic setup of IS-IS and the additional commands for fine-tuning the IS-IS processes**
- **Three main parts of a CLNS address (prefix, system ID, and NSEL)**
- **Interface commands for optimizing IS-IS to maximize its efficiency**
- **Route summarization in IS-IS**
- **Commands for verifying and troubleshooting the IP functionality of the Integrated IS-IS network**

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 5-17

References

For additional information, refer to these resources:

- RFC 995, *End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8437*.
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.
- Martey, A. *IS-IS Network Design Solutions*. Indianapolis, Indiana: Cisco Press; 2002.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 5-1: Configuring Integrated IS-IS in Multiple Areas

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) Place the IS-IS configuration steps in order.
- A) configure NET
 - B) enable IS-IS on the router
 - C) enable IS-IS on the interfaces
 - D) define areas and addressing
- Q2) The router identifies which interfaces participate in IS-IS routing by the _____.
A) **network** command
B) NET that is configured for each interface
C) **ip router isis** command
D) NET that is configured for each router
- Q3) IS-IS summarization allows you to _____.
A) summarize the list of NETs
B) summarize the area address
C) summarize a set of IP addresses into a less specific address
D) enumerate the IS and ES neighbors
- Q4) Which command shows the IS-IS neighbor routers?
A) **show ip protocols**
B) **show clns protocols**
C) **show ip route isis**
D) **show ip route**

Quiz Answer Key

Q1) 1-D, 2-B, 3-A, 4-C

Relates to: Integrated IS-IS Configuration Steps

Q2) C

Relates to: Basic IS-IS Configuration Commands

Q3) C

Relates to: Scalable IS-IS in Large Networks

Q4) A

Relates to: Verifying IS-IS Configuration and Troubleshooting IS-IS Operations

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:

- Quiz 5-1: Overview of IS-IS Routing and CLNS
- Quiz 5-2: Understanding CLNS Addressing
- Quiz 5-3: Basic Operations of IS-IS in a CLNS Environment
- Quiz 5-4: Basic Operations of Integrated IS-IS in an IP and CLNS Environment
- Quiz 5-5: Configuring Basic Integrated IS-IS

Quiz 5-1: Overview of IS-IS Routing and CLNS

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

Objectives

This assessment tests your knowledge of how to:

- Define the uses of Intermediate System-to-Intermediate System routing
- Explain how integrated Intermediate System-to-Intermediate System routing operates
- Explain how the End System-to-Intermediate System Discovery Protocol operates
- Differentiate between Open System Interconnection routing levels
- Compare IS-IS and Open Shortest Path First routing

Quiz

Answer these questions:

- Q1) Level 1 routing is responsible for which task?
- A) exchanging prefix information between areas
 - B) building topology of ES and IS in areas
 - C) using ES-IS to learn prefix information
 - D) CLNP routing
- Q2) Level 2 routing is responsible for which task?
- A) exchanging prefix information between areas
 - B) building topology of ES and IS in areas
 - C) using ES-IS to learn prefix information
 - D) CLNP routing
- Q3) Good IS-IS design features which two properties? (Choose two.)
- A) CLNS addresses confined to Level 1
 - B) begins with a summarizable address plan
 - C) two-level hierarchy
 - D) routers with minimal memory and CPU
- Q4) Which two characteristics describe IS-IS advantages over OSPF? (Choose two.)
- A) better support from the IETF
 - B) more documentation and support
 - C) ubiquitously implemented
 - D) support for CLNS
 - E) more extensible
 - F) faster convergence

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 5-2: Understanding CLNS Addressing

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

Objectives

This assessment tests your knowledge of how to:

- Define the Network Service Access Point address
- Define the Network Entity Title address

Quiz

Answer these questions:

- Q1) Which term describes an NSAP address?
- A) NASCAR address
 - B) CLNS address
 - C) protocol-specific port
 - D) replacement for BGP
- Q2) Which two statements are true with reference to CLNS? (Choose two.)
- A) Within an area, all system IDs must be unique.
 - B) Within an area, all area IDs (AFI, IDI, HO-DSP) must be identical.
 - C) Within an area, AFI and IDI must be identical, but HO-DSP may vary.
 - D) Within an area, all IP addresses must be in the same classful network.
- Q3) Which two terms are SNPAs? (Choose two.)
- A) MAC address
 - B) Frame Relay DLCI
 - C) IP address
 - D) CLNS address including NSEL
 - E) delivery point for traffic
- Q4) Which three conditions are system ID requirements? (Choose three.)
- A) must be 8 bytes
 - B) must be unique in an area
 - C) must be classless
 - D) must be unique in a routing domain
 - E) must be 6 bytes on a Cisco router

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 5-3: Basic Operations of IS-IS in a CLNS Environment

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

Objectives

This assessment tests your knowledge of how to:

- Explain router level definitions
- List the network topologies supported by Intermediate System-to-Intermediate System
- Describe adjacency behavior in a broadcast network
- Compare LAN, WAN, and Level 2 adjacencies
- Identify the types of link-state database synchronization

Quiz

Answer these questions:

- Q1) Which address component is used to identify the router in an IS-IS environment?
- A) SNPA
 - B) NRLI
 - C) NET
 - D) system number
- Q2) Which two network representations are supported by IS-IS?
(Choose two.)
- A) broadcast
 - B) NBMA
 - C) stub
 - D) general
 - E) NSSA
- Q3) What is a pseudonode?
- A) a representation of a Level 2 router in a Level 1 database
 - B) an ES that sometimes acts like an IS
 - C) an IS that sometimes acts like an ES
 - D) a DIS
- Q4) Which communication method is used by two Level 1 areas?
- A) tunnel
 - B) Level 1 runs on broadcast multiaccess networks
 - C) through Level 2
 - D) using PDUs

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 5-4: Basic Operations of Integrated IS-IS in an IP and CLNS Environment

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

Objectives

This assessment tests your knowledge of how to:

- Explain the purpose of Integrated Intermediate System-to-Intermediate System network entity title addressing for advertising IP networks
- Explain the path selection process for Intermediate System-to-Intermediate System routing
- Demonstrate how an IP forwarding database is constructed

Quiz

Answer these questions:

- Q1) Which address does integrated IS-IS require?
- A) IP address to use as router ID
 - B) IP addresses on interfaces
 - C) CLNS address to identify the device
 - D) CLNS addresses on interfaces
- Q2) Which two characteristics are true about Dijkstra calculations in IS-IS? (Choose two.)
- A) performs on separate Level 1 and Level 2 databases
 - B) performs on IP Type, Length, Value (TLV)
 - C) uses shortest path—lowest sum of link metrics
 - D) can be disabled
- Q3) Routing from 49.BAD1.1921.6800.0111.00 to 49.BAD7.1921.6800.0112.00 takes place at what level?
- A) Level 1
 - B) Level 2
 - C) not enough information to determine
 - D) routing not possible between these networks
- Q4) What is SNPA?
- A) the OSI specification for SPF
 - B) a data-link address
 - C) Level 2 routing
 - D) the interdomain component of IS-IS—not supported by Cisco routers

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 5-5: Configuring Basic Integrated IS-IS

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

Objectives

This assessment tests your knowledge of how to:

- Describe the configuration process for Integrated IS-IS in an IP environment
- Configure Intermediate System-to-Intermediate System routing with default settings
- Optimize IS-IS by adjusting the intermediate system type, circuit type, and metric
- Configure route summarization within Intermediate System-to-Intermediate System

Quiz

Answer these questions:

- Q1) What is the default IS-IS routing level of a Cisco router?
- A) 0
 - B) Level 1
 - C) Level 2
 - D) 3
 - E) Level 1-2
- Q2) A NET address is required to configure Integrated IS-IS for routing IP only.
- A) true
 - B) false
- Q3) To configure IS-IS on an interface, which command must be executed from configuration mode?
- A) **router isis**
 - B) **isis interface**
 - C) **ip router isis**
 - D) **is-type level-1**
- Q4) What is the default IS-IS metric for Fast Ethernet interfaces?
- A) 10
 - B) 16
 - C) 83
 - D) 100
- Q5) Scalability is achieved by_____.
- A) NET assignment
 - B) route summarization
 - C) controlling ES-IS
 - D) limiting IS-IS resynchronization issues

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 5-1: Overview of IS-IS Routing and CLNS

- Q1) B
- Q2) A
- Q3) B, C
- Q4) D, E

Quiz 5-2: Understanding CLNS Addressing

- Q1) C
- Q2) A, B
- Q3) A, B
- Q4) B, D, E

Quiz 5-3: Basic Operations of IS-IS in a CLNS Environment

- Q1) C
- Q2) A, D
- Q3) D
- Q4) C

Quiz 5-4: Basic Operations of Integrated IS-IS in an IP and CLNS Environment

- Q1) C
- Q2) A, C
- Q3) B
- Q4) B

Quiz 5-5: Configuring Basic Integrated IS-IS

- Q1) E
- Q2) B
- Q3) C
- Q4) A
- Q5) B

Module 6

Manipulating Routing Updates

Overview

This module discusses different means of controlling routing update information. Route redistribution interconnects networks that use multiple routing protocols. Methods of controlling information between these routing protocols include using filters, changing the administrative distance, and configuring metrics. This module discusses each of these methods and explains the configuration of policy-based routing using route maps.

Module Objectives

Upon completing this module, you will be able to apply the different means of controlling routing update information to the configuration of policy-based routing.

Module Objectives

Cisco.com

- **Describe migration and route selection between IP routing protocols**
- **Configure route redistribution between multiple IP routing protocols**
- **Configure dynamic routing protocol updates for passive interfaces and distribute lists**
- **Control routing updates and redistribution of route filtering using route maps**
- **Change the default administrative distance of certain routes**
- **Configure policy-based routing**

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- **Migration and Route Selection Between Multiple IP Routing Protocols**
- **Configuring and Verifying Route Redistribution**
- **Controlling Routing Update Traffic**
- **Using Route Maps to Control Routing Updates**
- **Using Administrative Distance to Influence the Route Selection Process**
- **Policy-Based Routing**
- **Lesson Assessments**

Migration and Route Selection Between Multiple IP Routing Protocols

Overview

This lesson describes migration from one routing protocol to another and how Cisco routers make route selections when multiple protocols are active in the network.

Relevance

Simple routing protocols work well for simple networks, but as networks grow and become more complex, it may be necessary to change routing protocols. Often the transition between routing protocols takes place gradually, so there are multiple routing protocols running in the network for variable lengths of time. This lesson examines several reasons for using more than one routing protocol. It is important to understand how to exchange routing information between these routing protocols and how Cisco routers operate in a multiple routing protocol environment.

Objectives

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

- Describe the principles and issues that are involved in migrating from one routing protocol to another
- List planning issues for new IP address allocation
- Describe how to migrate to a scalable IP addressing plan
- Describe how to migrate to a new routing protocol
- Explain why route redistribution is useful
- Compare the seed metrics that are used by different routing protocols
- List the considerations for implementing route redistribution

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge
- Knowledge of routing protocol operation and configuration of Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks

Outline

The outline lists the topics included in this lesson.

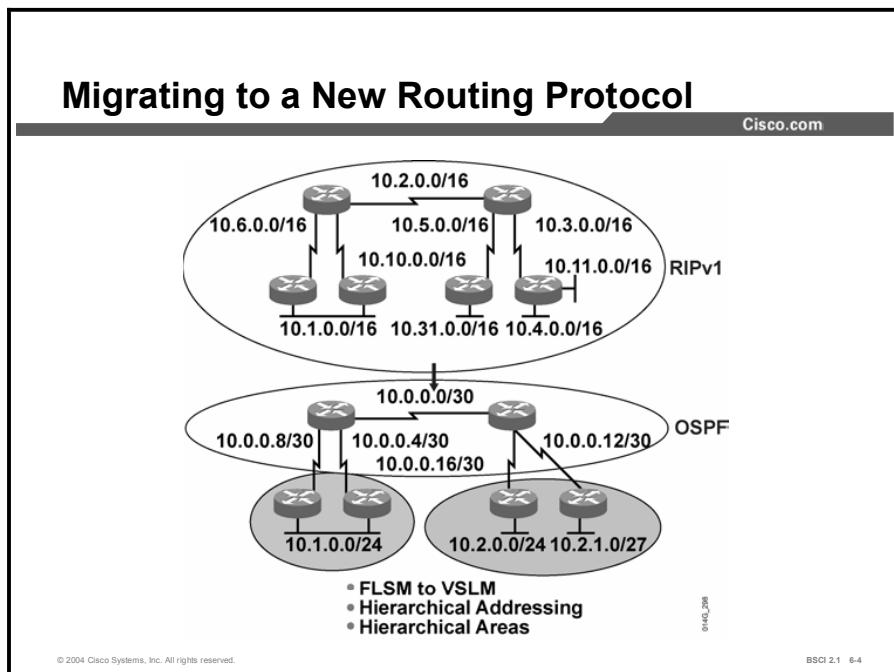
Outline

Cisco.com

- **Overview**
- **Considerations for Migrating to Another Routing Protocol**
- **Planning for New IP Address Allocation**
- **Procedures for Migrating to a New IP Address Space**
- **Migrating to a New Routing Protocol**
- **Purpose of Redistribution**
- **Seed Metrics**
- **Redistribution Implementation Considerations**
- **Summary**
- **Quiz**

Considerations for Migrating to Another Routing Protocol

This topic describes some of the principles and issues involved when you are migrating from one routing protocol to another.



There are many reasons why a change in routing protocols may be required. For example, as a network grows and becomes more complex, the original routing protocol may no longer be the best choice. Remember that Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) periodically send their entire routing tables in their updates.

As the network grows larger, the traffic from those updates can slow the network down, indicating that a change to a more scalable routing protocol may be necessary. Alternatively, perhaps you are using IGRP or Enhanced IGRP (EIGRP) and need a protocol that supports multiple vendors, or your company implements a policy that specifies a particular routing protocol.

Whatever the reason for the change, network administrators must conduct migration from one routing protocol to another carefully and thoughtfully. The new routing protocol will most likely have different requirements and capabilities from the old one.

It is important for network administrators to understand what must be changed and to create a detailed plan before making any changes. An accurate topology map of the network and an inventory of all network devices are also critical for success.

Link-state routing protocols, such as Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS), require a hierarchical network structure. Network administrators need to decide which routers will reside in the backbone area and how to divide the other routers into areas. While EIGRP does not require a hierarchical structure, it operates much more effectively within one.

During the transition, there will likely be a time when both routing protocols are running in the network. This may require redistribution of routing information between the two protocols. If so, carefully plan the redistribution strategy to avoid disrupting network traffic or causing suboptimal routing.

The timing of the migration must also be determined. Will the entire network change all at once or will sections change according to a timetable? Where will the migration start? An administrator must understand the network to make these decisions.

Example

In the preceding figure, the network was using RIP version 1 (RIPv1) and is migrating to OSPF. For the network administrator to be able to complete the migration, the following three changes are necessary:

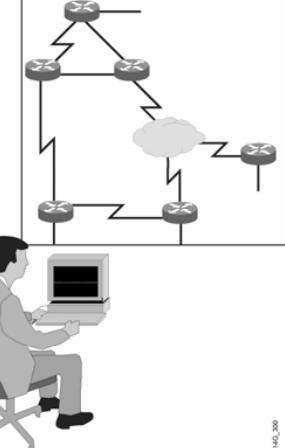
- Conversion of the old fixed-length subnet masking (FLSM) addressing scheme to a variable-length subnet masking (VLSM) configuration
- Use of a hierarchical addressing scheme to facilitate route summarization and make the network more scalable
- Division of the network into a transit backbone area and two other areas—when the network was using RIP, the network consisted of one large area

Planning for New IP Address Allocation

This topic examines the issues involved when you are planning for a new IP addressing scheme in the network.

Planning the IP Address Transition

Cisco.com



A diagram showing a network topology with several routers represented by circles with 'X' icons. One router is connected to a central switch-like node, which is then connected to another router. This second router is connected to a cloud icon representing the Internet, and finally to a host computer. A person is shown sitting at a desk, facing a computer monitor, representing someone planning the transition.

1. Decide if the transition is happening all at once or over an extended period of time and plan accordingly.
2. Decide on the new address space to be used for the entire network.
3. Allocate address space and document address assignment.
4. Examine and plan for the effect of the address changes on the following:
 - Secondary addresses
 - Network statement for routing
 - Host addressing
 - Access lists
 - NAT
 - DNS

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-5

One of the first steps when you are migrating to a new address space is to determine the time frame for the changeover. Is it going to be a gradual change with migration of different remote sites each weekend? Or is the new addressing going to take place all at one time? Additionally, consider resources and schedules when you are migrating multiple remote sites to a new address space.

The address plan created for the migration needs to be well-documented and accessible for reference by all internetworking personnel. If there are any questions or conflicts, this document will aid in settling the differences.

The plan should readdress the entire network and be reviewed by all internetworking personnel so that they can add comments or identify conflicts with existing addressing. The new address space may have portions already in use without the knowledge of the designer.

Having remote personnel review and agree to the address assignments for the entire network will prevent problems in the implementation stage.

Once the IP addressing scheme has been determined, you must plan its implementation. In most situations, the network must stay up during the transition from one protocol to another, and from one IP addressing plan to the other. For successful implementation, carefully consider the following areas:

- **Host addressing:** If host IP addresses are statically assigned, this is an excellent time to migrate using DHCP. If DHCP is already in use, then changes in IP addressing are transparent to most end users.

- **Access lists and other filters:** Firewalls and other types of traffic filters have been configured to use the old IP addresses. It is important to have complete documentation of all the traffic filters within the network so they can be updated to use the new IP addresses. If route filtering is based on the old addresses, then these filters will also need to be updated.
- **Network Address Translation (NAT):** If using NAT, configure it to recognize the new IP addresses as needing translation. Additionally, the new addresses may need to be translated to different outside addresses, depending on the network configuration.
- **Domain Name System (DNS):** If the network contains DNS servers, decide which mappings must be redone to reflect the new addresses.
- **Timing:** In a large network, changes are typically done in stages. You may start at the core and work outward, or start at the edges and work inward. Base the decision on a thorough knowledge of the network. Another important decision is the time of day and day of the week to make changes. Be sure to allow time to test and verify the new configuration.
- **Transition strategy:** Decide whether to totally change sections of the network to use only the new protocol and IP addressing or to run the new protocol and IP addresses in tandem with the old ones during the transition. If it is desirable to use both old and new IP addresses for a time, then you may need to configure secondary addresses on the routers.

Note Do not consider this list of planning considerations exhaustive.

Example

Suppose that a migration is being done from RIP to OSPF because there are frequent changes in the network. Frequent changes cause frequent RIP updates to be sent, which uses up bandwidth.

Additionally, the network convergence is slow with RIP. If OSPF is implemented in this network without changing the addressing to include route summarization, then triggered updates will still be sent frequently when the network topology changes.

The changes will cause the shortest path first (SPF) algorithm to be recomputed frequently, which in turn will disrupt routing. In this case, OSPF would probably be a worse choice than RIP.

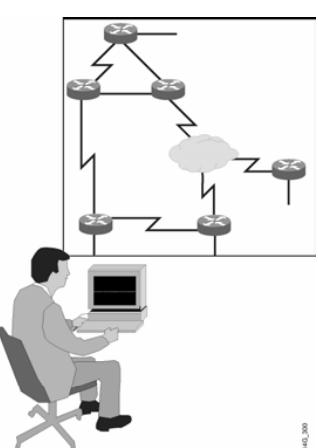
However, if a proper addressing plan were implemented, then this same network could run very efficiently. With route summarization in the right places, changes in the network topology would be hidden from most of the other routers and the SPF algorithm would not need to run with every flapping link.

Procedures for Migrating to a New IP Address Space

This topic describes how to implement a transition to new IP addressing after the initial planning phase is complete.

Implementing the IP Address Transition

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

1. Select the router and the subnet to be transitioned.
2. Assign secondary IP addresses to routers.
3. Assign new network statements to the routing process.
4. Update DNS for new addresses.
5. Implement DHCP, if not already used.
6. Configure DHCP server to assign new addresses, mask, and default gateways.
7. Allow enough time for transition.
8. Change secondary IP address to primary.
9. Remove old network statements from the routing process.
10. Remove old DNS entries.
11. Migrate to new routing protocol with redistribution.

0145_300

BSCI 2.1 6-6

Once the plans for transitioning to a new IP addressing scheme are complete, implementation must occur. Some of the tasks involved in implementation are as follows:

- **Host addressing:** Configure the DHCP server to start assigning the new IP addresses to individual hosts. Configure new static IP addresses on devices, such as servers. Also, remember to change the assigned default gateway.
- **Access lists and other filters:** It is important to keep complete and detailed documentation of all access lists, firewall configurations, routing updates, and other filters in the network. You must update all these elements so that they use the new IP address ranges.
If you are keeping the old and new address ranges active during the transition, then the access lists and filters will need modification to add the new addresses. After the transition is complete, you must remove the old addresses.
- **NAT:** It is also important to have complete documentation of all devices performing NAT within the network. Servers, routers, and firewall devices can all perform translation, and they may need to have their configurations changed.
If you are using both address ranges during the transition, then just add the new addresses. Again, if you use this approach after the transition is complete, you must go back and remove the old addresses.
- **DNS:** Any DNS used for internal addresses will need mappings for the new IP addresses. Be sure to include the changes for any static hosts, such as web or application servers.

- **Timing and transition strategy:** If some portions of the network will be using both the old and the new IP addresses for any length of time during the transition, then configure the affected routers to recognize and use both address ranges. One configuration is to use secondary addresses on the router interfaces.

The appropriate steps for the transition of IP address space may resemble the steps listed in the figure.

Configuring a Secondary IP Address

Cisco.com

Before:

```
Router# show run  
  
<output omitted>  
interface Ethernet0  
ip address 10.1.2.3 255.255.255.0
```

```
Router(config)# interface e0  
Router(config-if)# ip address 172.17.1.3 255.255.255.240 secondary
```

After:

```
Router# show run  
  
<output omitted>  
interface Ethernet0  
ip address 172.17.1.3 255.255.255.240 secondary  
ip address 10.1.2.3 255.255.255.0
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

The following figure illustrates how to configure a secondary IP address on an interface.

If secondary addresses are used, they require configuration before any of the host addressing, NAT, or access lists can be changed. The secondary address is the default gateway that the DHCP server assigns to hosts using the new addresses.

The old routing protocol may need updating to include the new networks in its network statements. You must update the old routing protocol if you want it to route for these networks.

Some issues are involved in using secondary addresses with some routing protocols. EIGRP and OSPF use the primary IP address as the source of their updates. EIGRP and OSPF expect the routers on both sides of a link to belong to the same subnet. They do not accept an update from a router on the wrong subnet or from a neighbor relationship with that router.

EIGRP generates error messages constantly in that situation. Therefore, remember to use the same subnet as the primary address on neighbor routers. Do not use a subnet as the secondary address on one router and the primary address on another.

When all routers in that portion of the network are using the new routing protocol and the new IP address ranges, reconfigure the routers to use the new IP addresses as primary.

A way to introduce more fault tolerance into this process is to configure the old addresses as secondary until the entire network has transitioned, everything has been tested, and the network is stable. In other words, swap the primary and secondary addresses.

The old addresses are now secondary, and the new addresses are primary. Remember to go back and remove the old IP addresses when they are no longer needed.

Migrating to a New Routing Protocol

After planning and implementing of the new IP addressing, the migration to the new routing protocol can begin. This topic describes how to accomplish the migration.

Migrating to a New IP Routing Protocol

Cisco.com

- **Implement and test the routing solution in the lab environment.**
- **Back up the router configurations.**
- **Determine the timeline for implementing and testing the new router configuration.**
- **Identify the boundary routers where the multiple routing protocols will run.**
- **Determine which routing protocol is the core and which is the edge.**
- **Determine the directions that you want to redistribute the protocols.**

What do I need to determine before configuring redistribution?



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-8

Before making any changes to the network, plan an escape route. Make sure that you have backup copies of all device configurations. The network documentation should include information on packet-flow paths so that you can be sure that the changes will not create suboptimal paths or routing loops. It should also include baseline values for data flow.

Additionally, you must verify that all devices support the new routing protocol. If not, you need to download, install, and test any required Cisco IOS software upgrades before beginning the migration.

Then, consider the impact of the changes on user traffic, and make changes when traffic is least likely to be affected. The migration strategy should be tested in as realistic an environment as possible to identify and correct any bugs ahead of time.

To avoid delays, you need to have a clear and comprehensive timeline for all steps in the migration. Be sure to allow time for testing and verifying changes as well as configuration. The migration to a new routing protocol is typically gradual: one section of the network at a time.

In planning the IP addressing for the network, you need to divide the network into either logical or physical hierarchical areas. A major task is to plan which areas will be migrated to the new protocol and when the migration will take place.

Usually, a choice must be made between starting the migration at the core of the network and working out to the edges, or starting at an edge router and working in toward the network core. Each approach has its pros and cons. If you start at an edge area, you can install and test the protocol without disrupting the main network traffic. Problems that may not have shown up in a

testing lab can be worked out in a more realistic environment before you go further with the migration.

Migrations to protocols that require a backbone area should begin at the core of the network. Because all interarea traffic goes through the backbone, the backbone must be in place before the areas can communicate.

Other reasons to begin with the network core include the fact that there are typically fewer devices at the core, and that redundancy is usually built into the core design, which helps minimize the effects of any problems. Additionally, the most experienced network staff is usually at the same location as the core network devices.

Part of migrating to a new routing protocol includes redistribution between the old and the new protocols. As part of the timeline, you must determine how many routers will be converted over to the new routing protocol at one time.

The routers that are the gateways between the old and the new routing protocols are the ones that may perform redistribution. The following two methods are available:

- **Two-way redistribution:** Redistribute all routes between the two routing processes.
- **One-way redistribution:** Pass a default route into the routing protocol on the edge of the network and redistribute only the networks learned from the routing protocol configured on the edge routers into the routing protocol running on the core routers.

Note Once migration has begun, be sure to test, verify, and document each step.

Purpose of Redistribution

This topic explains route redistribution and why it is useful.

Using Multiple Routing Protocols

Cisco.com

- **Interim during conversion**
- **Application-specific protocols**
 - One size does not always fit all
- **Political boundaries**
 - Groups that do not work well with others
- **Mismatch between devices**
 - Multivendor interoperability
 - Host-based routers

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-9

Multiple routing protocols may be necessary in the following situations:

- When you are migrating from an older Interior Gateway Protocol (IGP) to a new IGP. Multiple redistribution boundaries may exist until the new protocol has completely displaced the old protocol. Dual existence of protocols is effectively the same as a long-term coexistence design.
- When use of another protocol is desired, but the old routing protocol is needed for host systems; for example, UNIX host-based routers running RIP.
- Different departments might not want to upgrade their routers to support a new routing protocol.
- In a mixed-router vendor environment, you can use a Cisco-specific routing protocol like EIGRP in the Cisco portion of the network and a common standards-based routing protocol, like OSPF, to communicate with non-Cisco devices.

When multiple routing protocols are running in different parts of the network, there may be a need for hosts in one part of the network to reach hosts in the other part. One solution is to advertise a default route into each routing protocol, but that is not always the best policy. The network design may not allow default routes.

If there is more than one way to get to a destination network, routers may need information about routes in the other parts of the network to determine the best path to that destination. Additionally, if there are multiple paths, a router must have sufficient information to determine a loop-free path to the remote networks.

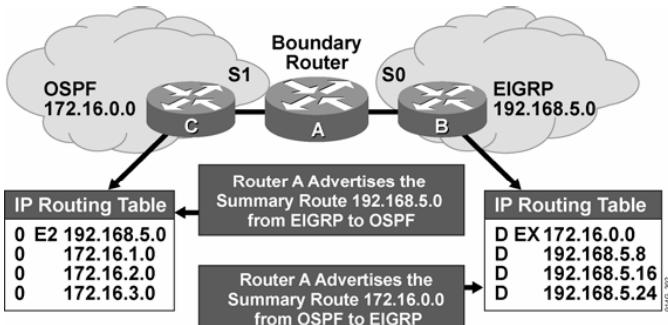
Cisco routers allow internetworks using different routing protocols, referred to as routing domains, or autonomous systems, to exchange routing information through a feature called route redistribution.

Redistribution is how routers connect different routing domains so that they can exchange and advertise routing information between the different autonomous systems.

Note The term “autonomous system (AS),” as used here, denotes internetworks using different routing protocols. These routing protocols may be IGP or Exterior Gateway Protocols (EGPs). This is a different use of the AS than when discussing the Border Gateway Protocol (BGP).

Redistributing Route Information

Cisco.com



- Routes are learned from another routing protocol when a router redistributes the information between the protocols.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-10

Within each AS, the internal routers have complete knowledge about their network. The router that interconnects the autonomous systems is called a boundary router. The boundary router must be running all the routing protocols that will be exchanging routes.

In most cases, route redistribution must be configured in order to redistribute routes from one routing protocol to another routing protocol. The only time that redistribution is automatic in IP routing protocols is between IGRP and EIGRP processes running on the same router and using the same AS number.

When a router redistributes routes, it allows a routing protocol to advertise routes that were not learned through that routing protocol. These redistributed routes could have been learned via a different routing protocol, such as when redistributing between EIGRP and OSPF. They also could have been learned from static routes or by a direct connection to a network.

Routers can redistribute static and connected routes as well as routes from other routing protocols.

Redistribution is always performed outbound. The router doing redistribution does not change its routing table. When, for instance, redistribution between OSPF and EIGRP is configured, the OSPF process on the boundary router will take the EIGRP routes in the routing table and advertise them as OSPF routes to its OSPF neighbors.

Likewise, the EIGRP process on the boundary router will take the OSPF routes in the routing table and advertise them as EIGRP routes to its EIGRP neighbors. Then both autonomous systems will know about the routes of the other, and each AS can then make informed routing decisions for these networks.

EIGRP neighbors use the EIGRP external (D EX) listing to route traffic destined for the other AS via the boundary router. The boundary router must have the OSPF routes for that destination network in its routing table to be able to forward the traffic.

For this reason, routes must be in the routing table in order for them to be redistributed. This requirement may seem self-evident, but it can be a source of confusion.

For instance, if a router learns about a network via EIGRP and OSPF, only the EIGRP route would be put in the routing table because it has a lower administrative distance. Suppose RIP is also running on this router and you want to redistribute OSPF routes into RIP. That network will not be redistributed into RIP because it is in the routing table as an EIGRP route, not as an OSPF route.

Example

The previous figure illustrates an AS running OSPF that is connected to an AS running EIGRP. The internal routers within each AS have complete knowledge about their networks, but they do not know about the routes present in the other AS. Router A is the boundary router, and it has OSPF and EIGRP processes active.

Without redistribution, router A is performing “ships that pass each other in the night” routing. Router A passes OSPF route updates to OSPF neighbors on the interfaces participating in OSPF routing. Router A also passes EIGRP route updates to EIGRP neighbors on the interfaces participating in EIGRP routing. Router A does not exchange information between EIGRP and OSPF.

If routers in the OSPF routing domain need to learn about the routes in the EIGRP domain or vice versa, then router A must redistribute routes between EIGRP and OSPF.

In the previous figure, router A learns about network 192.168.5.0 from router B via the EIGRP routing protocol running on its S0 interface. It redistributes that information to router C via OSPF on its S1 interface. Routing information is also passed in the other direction, from OSPF to EIGRP.

The routing table in router B shows that it has learned about network 172.16.0.0 via EIGRP (as indicated by the “D” in the routing table) and that the route is external to this AS (as indicated by the “EX” in the routing table).

The routing table in router C shows that it has learned about network 192.168.5.0 via OSPF (as indicated by the “O” in the routing table) and that the route is external (type 2) to this AS (as indicated by the “E2” in the routing table).

In this example, router A is redistributing a summary of the routes within its AS. This approach helps improve routing table stability and decreases the size of the routing tables.

Seed Metrics

When a router redistributes routing protocol information, it must assign a metric to the redistributed routes. This topic compares the seed metrics that are used by different routing protocols when performing redistribution.

Seed Metric

Cisco.com

- **The first, or seed, metric for a route is derived from being directly connected to a router interface.**
- **Use the default-metric command to establish the seed metric for the route or specify the metric when redistributing.**
- **Once a compatible metric is established, the metric will increase in increments just like any other route.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-11

When the router advertises a link directly connected to one of its interfaces, the initial, or seed, metric that is used is derived from the characteristics of that interface, and the metric increases in increments as the routing information is passed to other routers.

For OSPF, the seed metric is based on the bandwidth of the interface. For IS-IS, each interface has a default IS-IS metric of 10. For EIGRP and IGRP, the seed metric is based on the interface bandwidth and delay. For RIP, the seed metric starts with a hop count of 0 and increases in increments from router to router.

However, redistributed routes are not physically connected to a router; they are learned from other routing protocols. How many hops equal bandwidth? If a boundary router is to redistribute information between routing protocols, it must be able to translate the metric of one routing protocol into the metric of the other routing protocol.

For example, if a boundary router receives a RIP route, the route will have hop count as a metric. To redistribute the route into OSPF, the router must translate the hop count into a cost metric that the OSPF routers will understand.

This seed metric, also referred to as the default metric, is defined during redistribution configuration. Once the seed metric for a redistributed route is established, the metric will increase in increments normally within the AS.

Note	The exception to this rule is OSPF E2 routes, which hold their initial metric regardless of how far they are propagated across an AS.
-------------	---

The **default-metric** command, used in the routing process configuration mode, establishes the seed metric for all redistributed routes.

Cisco routers also allow the seed metric to be specified as part of the **redistribution** command, either with the *metric* option or by using a route map.

Whichever way it is done, the initial seed metric should be set to a value larger than the largest metric within the receiving AS to help prevent suboptimal routing and routing loops.

Default Seed Metrics

Cisco.com

Protocol	Default Seed Metric
RIP	infinity
IGRP/EIGRP	infinity
OSPF	20 for all except BGP, which is 1
IS-IS	0
BGP	BGP metric is set to IGP metric value.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-12

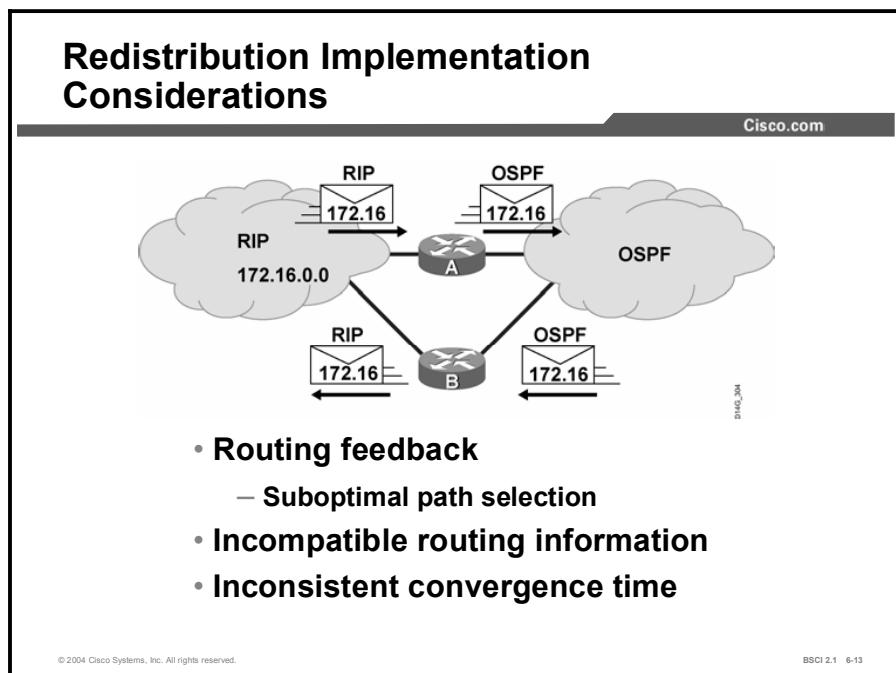
The figure illustrates that each IP routing protocol has a default seed metric value for redistributed routes. However, RIP, IGRP, and EIGRP do not advertise a redistributed route unless a seed metric is configured.

These protocols interpret the seed metric of 0 as infinity by default. A metric of infinity tells the router that the route is unreachable, and, therefore, it should not be advertised. Therefore, when redistributing routes into RIP, IGRP, and EIGRP, you must specify a default metric.

- For OSPF, the redistributed routes have a default type 2 metric of 20, except for redistributed BGP routes, which have a default type 2 metric of 1.
- For IS-IS, the redistributed routes have a default metric of 0. But unlike RIP, IGRP, or EIGRP, a seed metric of 0 will not be treated as unreachable by IS-IS.
- For BGP, the redistributed routes maintain the IGP routing metrics.

Redistribution Implementation Considerations

This topic describes some of the factors that must be considered before you implement redistribution in your network.



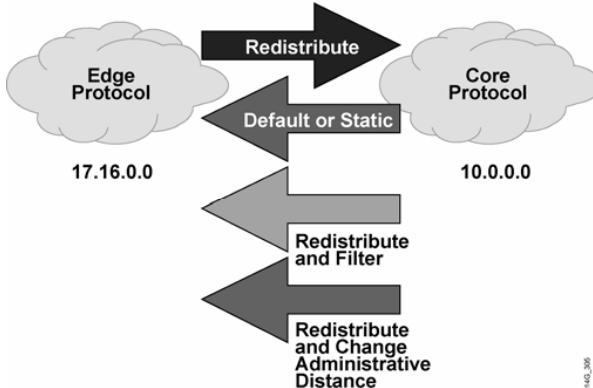
Redistribution of routing information adds to the complexity of a network and increases the potential for routing confusion, so it should be used only when necessary. The key issues that arise when you are using redistribution are the following:

- **Routing feedback (loops):** Depending on how you employ redistribution, routers can send routing information received from one AS back into that same AS. The feedback is similar to the routing loop problem that occurs in distance vector topologies.
 - **Incompatible routing information:** Because each routing protocol uses different metrics to determine the best path, path selection using the redistributed route information may be suboptimal. The metric information about a route cannot be translated exactly into a different protocol, so the path that a router chooses may not be the best.
- To prevent suboptimal routing, as a rule, you should assign to redistributed routes a seed metric that is higher than any routes that are native to the redistributing protocol. For instance, if RIP routes are being redistributed into OSPF and the highest OSPF metric is 50, the redistributed RIP routes should be assigned an OSPF metric higher than 50.
- **Inconsistent convergence time:** Different routing protocols converge at different rates. For example, RIP converges more slowly than EIGRP, so if a link goes down, the EIGRP network will learn about it before the RIP network.

Note Good planning will ensure that these issues do not cause problems in your network.

Redistribution Techniques

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-14

0145_306

The safest way to perform redistribution is to redistribute routes in only one direction, on only one boundary router within the network. To do this, you must first determine which routing protocol is the core routing protocol, and which ones are edge routing protocols.

The core routing protocol is the main routing protocol running in the network. During a transition between routing protocols, the core is the new routing protocol and the edge is the old routing protocol. In networks that run multiple routing protocols all the time, the core is usually the more advanced routing protocol.

If redistribution must be done in both directions, or on multiple boundary routers, then the redistribution should be tuned to avoid problems like suboptimal routing and routing loops.

Depending on your network design, you may use any of the following redistribution techniques:

- Redistribute a default route about the core AS into the edge AS. In one-way redistribution, routes from the edge routing protocols are redistributed into the core routing protocol, and a default route is sent back to the edge routers. This technique helps prevent route feedback, suboptimal routing, and routing loops.
- Redistribute multiple static routes about the core AS into the edge AS. The edge routes are still redistributed into the core, but static routes for the core networks are redistributed into the edge protocol and sent to the edge routers. This method works if there is one redistribution point only, but it may cause route feedback if there are multiple points.
- Redistribute routes from the core AS into the edge AS with filtering to block out inappropriate routes. For example, routes from the edge should not be redistributed back into the edge routers from the core via another redistribution point (when there are multiple boundary routers).
- Redistribute all routes from the core AS into the edge AS and from the edge AS into the core AS. Then modify the administrative distance that is associated with the external routes so that they are not the selected routes when multiple routes exist for the same destination.

In some cases, the route learned by the native (local) routing protocol is better, but it may have a higher (less believable) administrative distance. If two routing protocols advertise routes to the same destination, information from the routing protocol with the lowest administrative distance is placed in the routing table. A route redistributed into a routing protocol inherits the default administrative distance of that routing protocol by default.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Migration from one protocol to another requires a detailed plan, an accurate topology map of the network, and an inventory of all network devices.
- VLSM and scalability must be considered when you are changing the IP addresses in a network.
- Tasks involved in implementing a transition to new IP addressing after the initial planning phase are host addressing, access lists and other filters, NAT, DNS, and timing and transition strategy.
- Migration to a new routing protocol is typically gradual, one section of the network at a time.
- Redistribution allows routers to connect different routing domains so they can exchange and advertise routing information between the different autonomous systems.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-15

Summary (Cont.)

Cisco.com

- Redistribution allows a routing protocol to advertise routes that were not learned through that protocol.
- When the router advertises a link directly connected to one of its interfaces, the initial or seed metric used is derived from the characteristics of that interface, and the metric increments as the routing information is passed to other routers.
- Redistribution of routing information adds to the complexity of a network and increases the potential for routing confusion. Routing feedback, incompatible routing information, and inconsistent convergence time are the key issues that arise when you are using redistribution.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-16

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 three considerations when you are changing routing protocols? (Choose three.)
- A) needing a new IP addressing scheme
 - B) dividing the network into hierarchical areas
 - C) maintaining an existing FLSM environment
 - D) planning for route summarization
- Q2) Which three components should an efficient IP addressing plan include? (Choose three.)
- A) the same subnet mask for every network
 - B) the ability to summarize IP addresses
 - C) allocation of only the necessary amount of IP addresses per subnet
 - D) a hierarchical plan
- Q3) Which three configurations typically need to be reconfigured during the migration from one routing protocol to another? (Choose three.)
- A) access lists
 - B) NAT translations
 - C) host addressing
 - D) WAN connection type
- Q4) Which two statements concerning secondary addresses are true? (Choose two.)
- A) You can use secondary addresses when you are transitioning from one IP addressing scheme to another.
 - B) DHCP will automatically detect secondary addresses.
 - C) NAT cannot be used with secondary addresses.
 - D) Routing protocols do not use secondary addresses as the source of their routing updates.

- Q5) Place the steps in migrating to a new routing protocol in the correct order.
- A) _____ Back up the router configurations.
 - B) _____ Determine which routing protocol is the core and which is the edge.
 - C) _____ Identify the boundary routers where the multiple routing protocols will run.
 - D) _____ Implement and test the routing solution in the lab environment.
 - E) _____ Determine the directions in which you want to redistribute the protocols.
 - F) _____ Determine the time line for implementing and testing the new router configuration.
- Q6) Which three situations might require multiple routing protocols in a network? (Choose three.)
- A) when a new Layer 2-only switch is added to the network
 - B) when you are migrating from one routing protocol to another
 - C) when you are using routers from multiple vendors
 - D) when there are host-based routers that use a specific routing protocol
- Q7) Which three statements about redistribution of routing information between routing protocols are true? (Choose three.)
- A) provides reachability to networks in the remote routing domain
 - B) requires that both routing protocols be running on all routers
 - C) allows routers to make more informed routing decisions
 - D) allows routers to advertise routes learned from another source
- Q8) Which routing process configuration command is used to establish the seed metric for all redistributed routes?
- A) **default-metric**
 - B) **metric**
 - C) **seed-metric**
 - D) **cost**
 - E) **bandwidth**
- Q9) What is the safest way to perform route redistribution?
- A) one-way from the edge routers to the core
 - B) one-way from the core to the edge routers
 - C) two-way between all edge and core routers
 - D) two-way between all edge and core routers, but make the administrative distance of every protocol the same

Quiz Answer Key

- Q1) A, B, D
Relates to: Considerations For Migrating to Another Routing Protocol
- Q2) B, C, D
Relates to: Planning for New IP Address Allocation
- Q3) A, B, C
Relates to: Planning for New IP Address Allocation
- Q4) A, D
Relates to: Procedures for Migrating to a New IP Address Space
- Q5) A-2, B-5, C-4, D-1, E,-6, F-3
Relates to: Migrating to a New Routing Protocol
- Q6) B, C, D
Relates to: Purpose of Redistribution
- Q7) A, C, D
Relates to: Purpose of Redistribution
- Q8) A
Relates to: Seed Metrics
- Q9) A
Relates to: Redistribution Implementation Considerations

Configuring and Verifying Route Redistribution

Overview

This lesson describes how to configure route redistribution between various Interior Gateway Protocol (IGP) routing protocols. The commands for each protocol are covered. These commands differ slightly, according to the different routing protocol requirements. In addition, the impact of route redistribution is analyzed.

Relevance

Configuring route redistribution can be simple or complex, depending on the mix of routing protocols that you want to redistribute. The commands that are used to enable redistribution and to assign metrics vary slightly depending on the routing protocols being redistributed. Before configuring the exchange of routing information between routing protocols, you must understand the procedures for and requirements of each routing protocol. Redistribution must be configured correctly for each routing protocol to obtain proper results.

Objectives

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

- Describe how to configure route redistribution
- Use the **redistribute** command for RIP
- Use the **redistribute** command for OSPF
- Use the **redistribute** command for EIGRP
- Use the **redistribute** command for IS-IS
- Verify route redistribution operations by inspecting the resulting routing tables

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge
- Knowledge of routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Configuring Redistribution**
- **The redistribute Command for RIP**
- **The redistribute Command for OSPF**
- **The redistribute Command for EIGRP**
- **The redistribute Command for IS-IS**
- **Example of Implementing and Verifying Route Redistribution**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 6-3

Configuring Redistribution

This topic describes how to configure route redistribution in generic terms.

Redistribution Supports All Protocols

Cisco.com

```
RtrA(config-router)# redistribute ?
bgp      Border Gateway Protocol (BGP)
connected Connected
egp      Exterior Gateway Protocol (EGP)
eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
igrp     Interior Gateway Routing Protocol (IGRP)
isis     ISO IS-IS
iso-igrp IGRP for OSI networks
mobile   Mobile routes
odr      On Demand stub Routes
ospf    Open Shortest Path First (OSPF)
rip     Routing Information Protocol (RIP)
static   Static routes
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-4

As shown in the figure, redistribution supports all routing protocols. Additionally, static and connected routes can be redistributed to allow the routing protocol to advertise the routes without using a network statement for them.

Routes are redistributed into a routing protocol, and so the **redistribute** command is given under the routing process that is to receive the routes. Before implementing redistribution, consider the following points:

- Only protocols that support the same protocol stack are redistributed. For example, you can redistribute between IP RIP and OSPF because they both support the TCP/IP stack.
You cannot redistribute between Internetwork Packet Exchange (IPX) RIP and OSPF because IPX RIP supports the IPX/Sequenced Packet Exchange (SPX) stack and OSPF does not. Although there are different protocol-dependent modules of EIGRP for IP, IPX, and AppleTalk, routes cannot be redistributed between them because each protocol-dependent module supports a different protocol stack.
- The method used to configure redistribution varies slightly among different routing protocols and combinations of routing protocols. For example, redistribution occurs automatically between IGRP and EIGRP when they have the same AS number; however, redistribution must be configured between all other routing protocols. Some routing protocols require a metric to be configured during redistribution, but others do not.

The following generic steps apply to all routing protocol combinations. However, the commands that are used to implement these steps may vary. For configuration commands, it is important that you review the Cisco IOS documentation for the specific routing protocols that need to be redistributed.

Note	In this topic, the terms “core” and “edge” are generic terms that are used to simplify the discussion about redistribution.
-------------	---

- Step 1** Locate the boundary router that requires configuration of redistribution. Selecting a single router for redistribution minimizes the likelihood of creating routing loops that are caused by feedback.
- Step 2** Determine which routing protocol is the core or backbone protocol. Typically, this protocol is OSPF, IS-IS, or EIGRP.
- Step 3** Determine which routing protocol is the edge or short-term (in the case of migration) protocol. Determine if all routes from the edge protocol need to be propagated into the core. Consider methods that reduce the number of routes.
- Step 4** Select a method for injecting the required edge protocol routes into the core. Simple redistribution using summaries at network boundaries minimizes the number of new entries in the routing table of the core routers.

Once you have planned the edge-to-core redistribution, consider how to inject the core routing information into the edge protocol. Your choice depends on your network.

The redistribute Command for RIP

This topic examines the command for redistributing routes into RIP.

Configuring Redistribution into RIP

Cisco.com

```
RtrA(config)# router rip
RtrA(config-router)# redistribute ospf ?
<1-65535> Process ID
RtrA(config-router)# redistribute ospf 1 ?

match      Redistribution of OSPF routes
metric     Metric for redistributed routes
route-map  Route map reference
...
<cr>
```

- Default metric is infinity.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-5

Use the following command to redistribute routes into RIP:

```
Router(config-router)# redistribute protocol [process-id]
[match route-type] [metric metric-value] [route-map map-tag]
```

This figure shows how to configure for redistribution from OSPF process 1 into RIP.

In the figure, the example uses the **router rip** command to access the routing process into which routes need to be redistributed. In this case, it is the RIP routing process.

The example uses the **redistribute** command to specify the routing protocol to be redistributed into RIP. In this case, it is the OSPF routing process number 1.

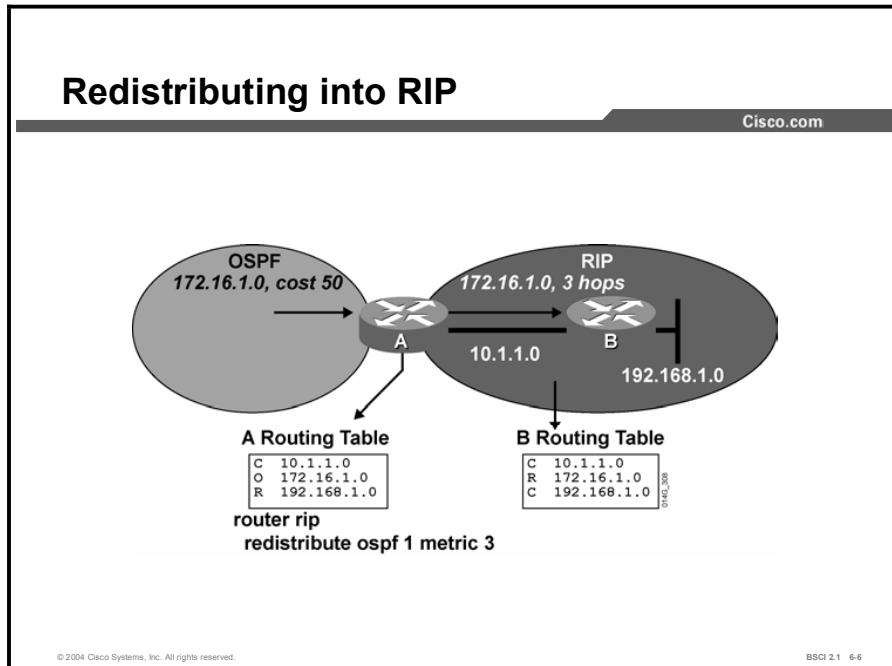
Note	The default metric is infinity except when you are redistributing a static or connected route. In that case, the default metric is 1.
-------------	---

The following table details the parameters of the **redistribute** command.

Table 1: The redistribute Command Parameters

Parameters	Description
<i>protocol</i>	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected , bgp , eigrp , egp , igrp , isis , iso-igrp , mobile , odr , ospf , static , or rip .
<i>process-id</i>	For BGP, EGP, EIGRP, or IGRP, this value is an AS number. For OSPF, this value is an OSPF process ID.
match <i>route-type</i>	(Optional) Command parameter used for redistributing OSPF routes into another routing protocol. For OSPF, the criterion by which OSPF routes are redistributed into other routing domains. It can be any of the following: <ul style="list-style-type: none"> ■ internal: Redistributions routes that are internal to a specific AS. ■ external 1: Redistributions routes that are external to the AS, but are imported into OSPF as a type 1 external route. ■ external 2: Redistributions routes that are external to the AS, but are imported into OSPF as a type 2 external route.
metric <i>metric-value</i>	(Optional) Parameter used to specify the RIP seed metric for the redistributed route. When you are redistributing into protocols other than OSPF (including RIP), if this value is not specified and no value is specified using the default-metric router configuration command, then the default metric is 0, which is interpreted as infinity, and routes will not be redistributed. The metric for RIP is the hop count.
route-map <i>map-tag</i>	(Optional) Identifier of a configured route map to be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol.

Example



In the figure, routes from OSPF process number 1 are being redistributed into RIP and given a seed metric of 3. Because no route type is specified, both internal and external OSPF routes are redistributed into RIP.

The redistribute Command for OSPF

This topic describes the commands and options for redistributing routes into OSPF.

Configuring Redistribution into OSPF

Cisco.com

```
RtrA(config)# router ospf 1
RtrA(config-router)# redistribute eigrp ?
<1-65535> Autonomous system number
RtrA(config-router)# redistribute eigrp 100 ?

metric      Metric for redistributed routes
metric-type OSPF/IS-IS exterior metric type for redistributed routes
route-map   Route map reference
subnets     Consider subnets for redistribution into OSPF
tag         Set tag for routes redistributed into OSPF
...
<cr>
```

- **Default metric is 20.**
- **Default metric type is 2.**
- **Subnets do not redistribute by default.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

Use the following command to redistribute routes into OSPF.

```
Router(config-router)# redistribute protocol [process-id]
[metric metric-value] [metric-type type-value] [route-map map-
tag] [subnets] [tag tag-value]
```

The figure shows how to configure for redistribution from EIGRP AS 100 into OSPF. It uses the **router ospf 1** command to access the OSPF routing process into which routes need to be redistributed. In this case, it is OSPF routing process 1.

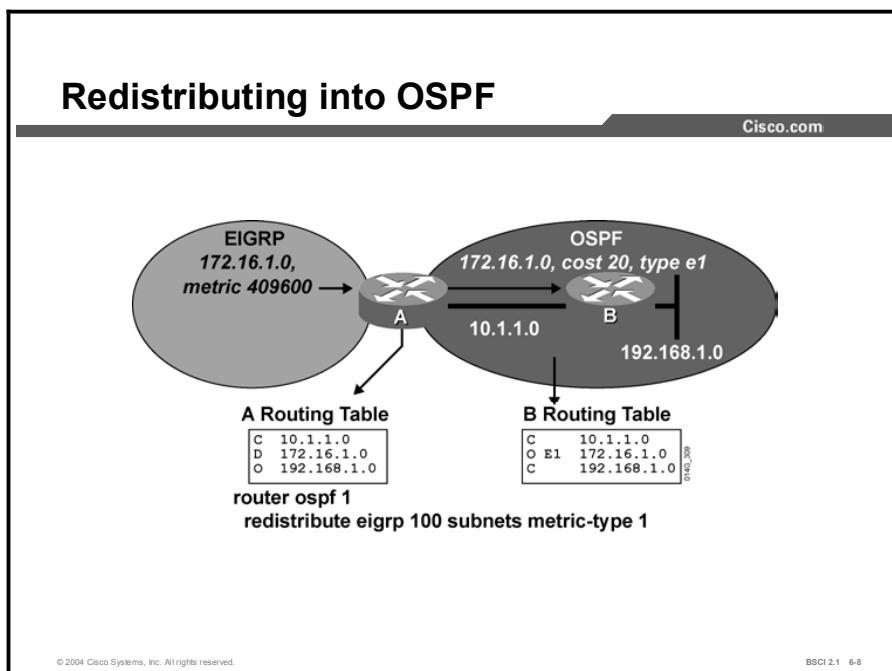
The figure uses the **redistribute** command to specify the routing protocol to be redistributed into OSPF. In this case, it is the EIGRP routing process for AS 100.

The following table details more of the parameters of the **redistribute** command.

Table 2: The redistribute Command Parameters

Parameters	Description
protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected , bgp , eigrp , egp , igrp , isis , iso-igrp , mobile , odr , ospf , static , or rip .
process-id	For BGP, EGP, EIGRP, or IGRP, this value is an AS number. For OSPF, this value is an OSPF process ID.
metric metric-value	(Optional) Parameter that specifies the OSPF seed metric that is used for the redistributed route. When you are redistributing into OSPF, the default metric is 20 (except for BGP, which is 1). Use a value consistent with the destination protocol, in this case, the OSPF cost.
metric-type type-value	(Optional) OSPF parameter that specifies the external link type that is associated with the external route that is advertised into the OSPF routing domain. This value can be 1 for type 1 external routes or 2 for type 2 external routes. The default is 2.
route-map map-tag	(Optional) Identifier of a configured route map to be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol.
subnets	(Optional) OSPF parameter that specifies that subnetted routes should be redistributed also. Only routes that are not subnetted are redistributed if the subnets keyword is not specified.
tag tag-value	(Optional) 32-bit decimal value that is attached to each external route. The OSPF protocol does not use this parameter. It may be used to communicate information between AS boundary routers (ASBRs).

Example



In the figure, the default metric of 20 for OSPF is being used, and the metric type is set to *external 1*. This setting means that the metric increases in increments whenever updates are passed through the network. The command contains the **subnets** option, so subnets are redistributed.

The redistribute Command for EIGRP

This topic describes the commands and options for redistributing routes into EIGRP.

Configuring Redistribution into EIGRP

Cisco.com

```
RtrA(config)# router eigrp 100
RtrA(config-router)# redistribute ospf ?
<1-65535> Process ID
RtrA(config-router)# redistribute ospf 1 ?

  match      Redistribution of OSPF routes
  metric    Metric for redistributed routes
  route-map  Route map reference
...
<cr>
```

- Default metric is infinity.

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 6-9

Use the following command to redistribute routes into EIGRP:

```
router(config-router)# redistribute protocol [process-id]
[match {internal | external 1 | external 2}] [metric metric-
value] [route-map map-tag]
```

The figure shows how to configure for redistribution from OSPF into EIGRP AS 100. It uses the **router eigrp 100** command to access the routing process into which routes need to be redistributed. In this case, it is the EIGRP routing process for AS 100.

The figure uses the **redistribute** command to specify the routing protocol to be redistributed into EIGRP AS 100. In this case, it is OSPF routing process 1.

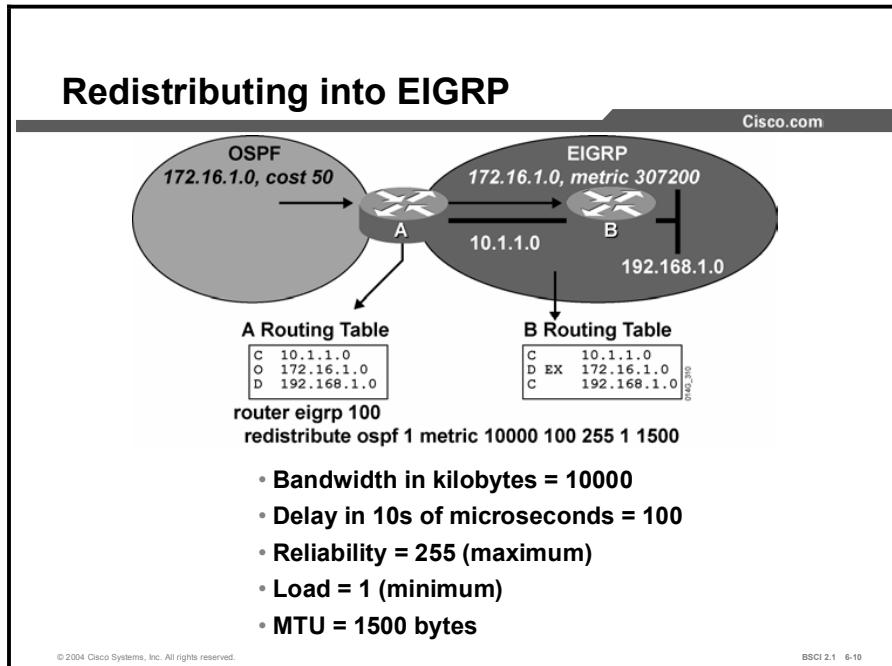
Note When you are redistributing a static or connected route into EIGRP, the default metric is equal to the metric of the associated interface.

The following table details the parameters of the **redistribute** command.

Table 3: The redistribute Command Parameters

Parameters	Description
protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected , bgp , eigrp , egp , igrp , isis , iso-igrp , mobile , odr , ospf , static , or rip .
process-id	For BGP, EGP, EIGRP, or IGRP, this value is an AS number. For OSPF, this value is an OSPF process ID.
match	(Optional) For OSPF, the criterion by which OSPF routes are redistributed into other routing domains. It can be one of the following: <ul style="list-style-type: none"> ■ internal: Redistributions routes that are internal to a specific AS. ■ external 1: Redistributions routes that are external to the AS but are imported into OSPF as a type 1 external route. ■ external 2: Redistributions routes that are external to the AS but are imported into OSPF as a type 2 external route.
metric metric-value	(Optional) Parameter that specifies the EIGRP seed metric, in the order of bandwidth, delay, reliability, load, and maximum transmission unit (MTU), for the redistributed route. When you are redistributing into protocols other than OSPF (including EIGRP), if this value is not specified and no value is specified using the default-metric router configuration command, the default metric is 0, zero is interpreted as infinity, and routes are not redistributed. Use a value consistent with the destination protocol. The metric for EIGRP is calculated based only on bandwidth and delay by default.
route-map map-tag	(Optional) Identifier of a configured route map that is interrogated to filter the importation of routes from this source routing protocol to the current routing protocol.

Example



In the figure, routes from OSPF process number 1 are redistributed into EIGRP AS 100. In this case, a metric is specified to ensure that routes are redistributed. The redistributed routes appear in the table of router B as external EIGRP (D EX) routes.

External EIGRP routes have a higher administrative distance than internal EIGRP (D) routes, so internal EIGRP routes are preferred over external EIGRP routes.

The redistribute Command for IS-IS

This topic describes the commands and options for redistributing routes into IS-IS.

Configuring Redistribution into IS-IS

Cisco.com

```
RtrA(config)# router isis
RtrA(config-router)# redistribute eigrp 100 ?

level-1      IS-IS level-1 routes only
level-1-2    IS-IS level-1 and level-2 routes
level-2      IS-IS level-2 routes only
metric        Metric for redistributed routes
metric-type   OSPF/IS-IS exterior metric type for redistributed routes
route-map     Route map reference
...
<cr>
```

- Routes are introduced as level 2 with a metric of 0 by default.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-11

Use the following command to redistribute routes into IS-IS:

```
router(config-router)# redistribute protocol [process-id]
[level level-value] [metric metric-value] [metric-type type-
value] [route-map map-tag]
```

The figure shows how to configure for redistribution from EIGRP AS 100 into IS-IS. It uses the **router isis** command to access the routing process into which routes need to be redistributed. In this case, it is the IS-IS routing process.

The figure uses the **redistribute** command to specify the routing protocol to be redistributed into IS-IS. In this case, it is the EIGRP routing process for AS 100.

The following table details the parameters of the **redistribute** command.

Table 4: The redistribute Command Parameters

Parameter	Description
protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected , bgp , eigrp , egp , igrp , isis , iso-igrp , mobile , odr , ospf , static , or rip .
process-id	For BGP, EGP, EIGRP, or IGRP, this value is an AS number. For OSPF, this value is an OSPF process ID.
level level-value	Redistributes external routes as level 1 (level-1), level 1 and level 2 (level-1-2), or level 2 (level-2) routes. The default is level 2.
metric metric-value	Specifies the IS-IS seed metric that is used for the redistributed route. IS-IS uses a default metric of 0. Unlike RIP, IGRP, and EIGRP, a default metric of 0 is not treated as unreachable, and is redistributed. The metric is increased in increments as the route is propagated into the IS-IS domain. Use a value consistent with the destination protocol, in this case the IS-IS cost.
metric-type type-value	Specifies the IS-IS metric type as external or internal. The default is internal.
route-map map-tag	(Optional) Identifier of a configured route map to be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol.

When redistributing IS-IS routes into other routing protocols, you have the option to include level 1, level 2, or both level 1 and level 2 routes. The following output shows the commands for choosing these routes. If no level is specified, then all routes are redistributed.

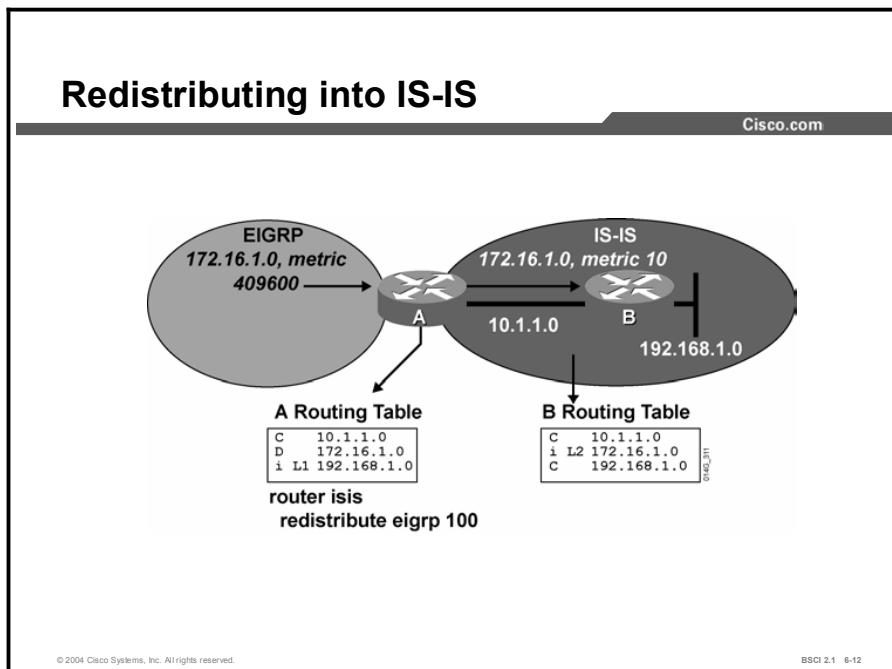
```

Router(config)# router ospf 1
Router(config-router)# redistribute isis ?

      level-1           IS-IS level-1 routes only
      level-1-2         IS-IS level-1 and level-2 routes
      level-2           IS-IS level-2 routes only

```

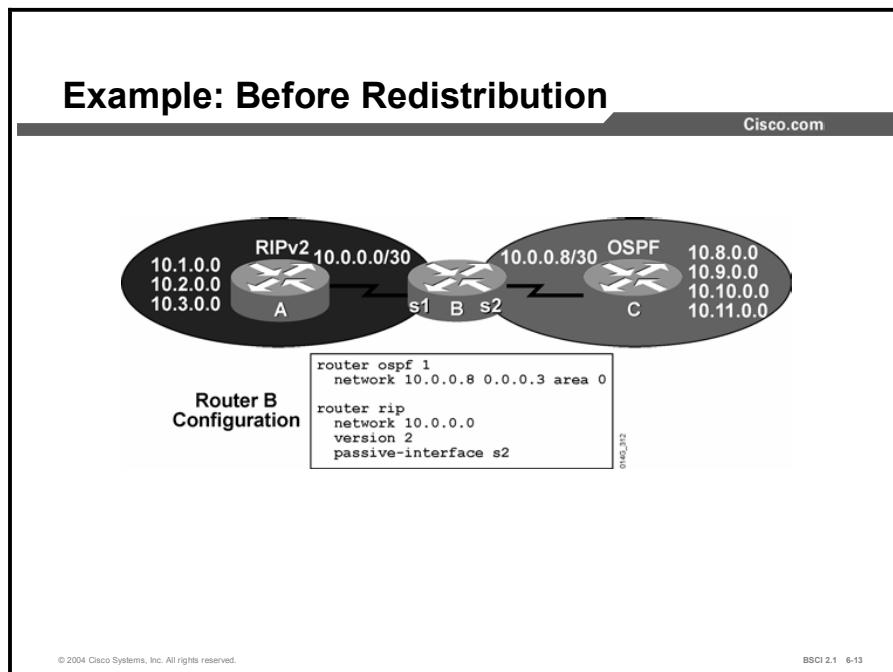
Example



In the figure, routes are redistributed from EIGRP AS 100 into IS-IS on router A. No metric is given, so these routes have a seed metric of 0. No level type is given, so the routes are redistributed as level 2 routes (as displayed in the router B routing table).

Example of Implementing and Verifying Route Redistribution

This topic combines the knowledge and techniques that were discussed in previous topics to show an example of route redistribution in a complex network using multiple routing protocols.



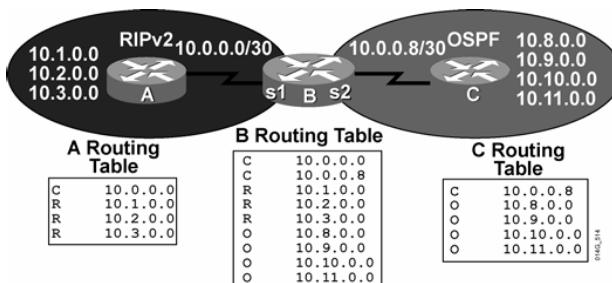
The figure shows the network of a hypothetical company. The network begins with two routing domains, or autonomous systems, one using OSPF and one using RIP version 2 (RIPv2). Router B is the boundary router. It connects directly to one router within each routing domain and runs both protocols.

Router A is in the RIP domain, and is advertising subnets 10.1.0.0, 10.2.0.0, and 10.3.0.0 to router B. Router C is in the OSPF domain and is advertising subnets 10.8.0.0, 10.9.0.0, 10.10.0.0, and 10.11.0.0 to router B.

The configuration of router B is shown in the figure. RIP is required to run on the serial 1 interface only. Therefore, the **passive-interface** command is given for interface serial 2. The **passive-interface** command prevents RIP from sending route advertisements out that interface. OSPF is configured on serial 2.

Example: Before Redistribution (Cont.)

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-14

The figure shows the routing tables of routers A, B, and C. Each routing domain is separate, and routers within them recognize routes that are communicated from their own routing protocols only.

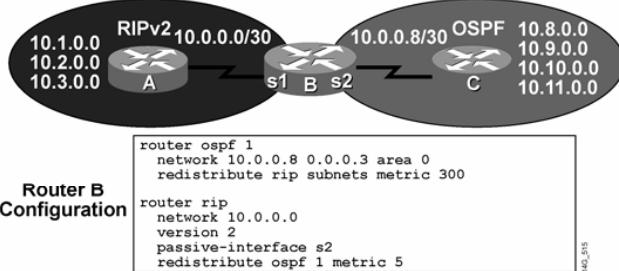
The only router with information on all the routes is router B, which is the boundary router that runs both routing protocols and connects to both routing domains.

The goal of redistribution in this network is for all routers to recognize all routes within the company. To accomplish this goal, the following redistribution is planned:

- Redistribute RIP routes into OSPF
- Redistribute OSPF routes into the RIP domain

Example: Configuring Redistribution at Router B

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-15

Router B is the boundary router, so redistribution is configured on it. The figure shows how router B is configured to accomplish the required redistribution.

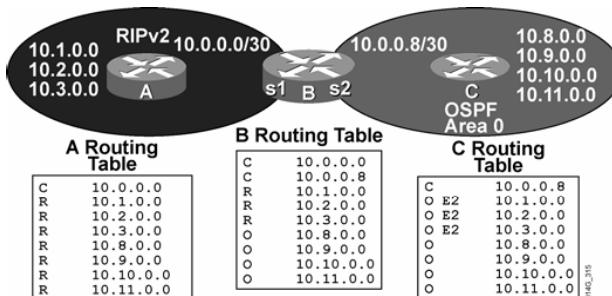
RIP is redistributed under the OSPF process. In this example, the metric is set under the **redistribution** command. Other options include specifying a default metric or accepting the OSPF default metric of 20.

The **default-metric** command assigns a seed metric to all routes redistributed into OSPF from any origin. If a metric value is configured under a specific **redistribution** command, this value overrides the default metric value. A value of 300 is selected because it is a worse metric than any of the native OSPF routes.

Under the RIP process, routes are redistributed in from OSPF process number 1. These routes are redistributed into RIP with a metric of 5. A value of 5 is chosen because it is higher than any metric in the RIP network.

Example: Routing Tables After Route Redistribution

Cisco.com



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-18

The figure shows the routing tables of all three routers after redistribution is completed. The goal is accomplished. All routers now have routes to all remote subnets. There is complete reachability within the entire network.

However, routers A and C now have many more routes to keep track of than before. Each router is also affected by topology changes in the routing domain of the other router.

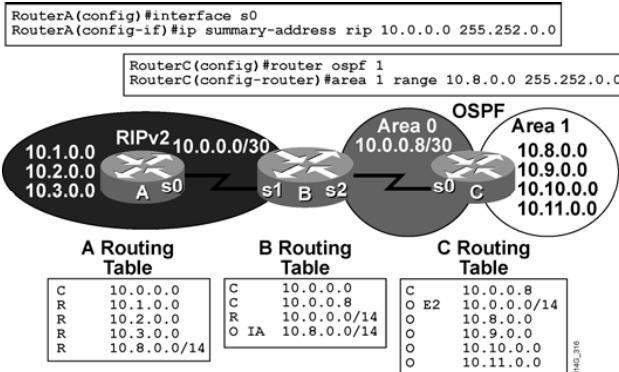
Depending on network requirements, you can increase efficiency by summarizing the routes before redistributing them. Remember that route summarization hides information.

If routers in the other autonomous systems are required to track topology changes within the network, then route summarization should not be performed, because it hides information that the routers need.

A more typical case is that the routers need to recognize topology changes only within their own routing domains. In this case, performing route summarization is appropriate.

Example: Routing Tables After Summarizing Routes and Redistributions

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-17

If routes are summarized before redistribution, then the routing tables of each router are significantly smaller. Router B benefits the most; it now has only four routes to keep track of instead of nine. Router A has five routes instead of eight, and router C has six routes to keep track of instead of eight.

The following commands are used to summarize routes for each protocol:

- **Router A, RIP:** For RIPv2, the summarization command is given at the interface connecting router B with router A. This summary address is advertised out of that interface instead of the individual subnets. One limitation of RIP is that the subnet mask of the summary address must be greater than or equal to the default mask for the major classful network. Use the following summarization command for RIPv2:

```
RouterA(config)# interface s0
RouterA(config-if)# ip summary-address rip 10.0.0.0
255.252.0.0
```

- **Router C, OSPF:** You must perform summarization in OSPF at an area border router (ABR) or an ASBR. Create another OSPF area that includes the four subnets to be summarized. Give the command for summarization under the OSPF process at router C, which becomes an ABR. Use the following summarization command for OSPF:

```
RouterC(config)# router ospf 1
RouterC(config-router)# area 1 range 10.8.0.0 255.252.0.0
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Redistribution supports all protocols and allows the routing protocols to advertise the routes without using a network statement for them. Routes are redistributed into a routing protocol. The redistribute command is given under the routing process that is to receive the routes.**
- **The router rip and redistribute commands are used to redistribute routes into RIP.**
- **The router ospf and redistribute commands are used to redistribute routes into OSPF.**
- **The router eigrp and redistribute commands are used to redistribute routes into EIGRP.**
- **The router isis and redistribute commands are used to redistribute routes into IS-IS.**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 6-18

References

For additional information, refer to these resources:

The command reference and configuration documentation guides on Cisco.com at
<http://www.cisco.com/univercd/home/home.html>

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) Redistribution can be configured between which two protocols? (Choose two.)
- A) IP RIP and IPX RIP
 - B) IPX EIGRP and AppleTalk EIGRP
 - C) IGRP and OSPF
 - D) IP RIP and EIGRP
- Q2) Which two options are available when you are redistributing routes into RIP? (Choose two.)
- A) specifying a metric
 - B) calling a route map to modify the redistribution
 - C) tagging the redistributed routes with a value
 - D) redistributing all subnets with the **subnet** command
- Q3) If no metric type is specified when routes are redistributed into OSPF, what is the default behavior of the router?
- A) uses a metric type of E1
 - B) uses a metric type of E2
 - C) prompts for a metric type with the “incomplete command” message
 - D) does not redistribute the route
- Q4) If no metric is specified when routes are redistributed into EIGRP, what is the default behavior of the router?
- A) assigns a default metric of 1
 - B) assigns a default metric of 20
 - C) prompts for a metric with the “incomplete command” message
 - D) does not redistribute the route
- Q5) If no level is specified when routes are redistributed into IS-IS, what is the default behavior of the router?
- A) redistributes the routes as level 1 routes
 - B) redistributes the routes as level 2 routes
 - C) redistributes the routes as level 1 and level 2 routes
 - D) does not redistribute the routes

- Q6) The **subnet** keyword is required when you are redistributing subnet routes into which routing protocol?
- A) OSPF
 - B) RIP
 - C) EIGRP
 - D) IS-IS

Quiz Answer Key

Q1) C, D

Relates to: Configuring Redistribution

Q2) A, B

Relates to: The redistribute Command for RIP

Q3) B

Relates to: The redistribute Command for OSPF

Q4) D

Relates to: The redistribute Command for EIGRP

Q5) B

Relates to: The redistribute Command for IS-IS

Q6) A

Relates to: Example of Implementing and Verifying Route Redistribution

Controlling Routing Update Traffic

Overview

This lesson discusses how to control the updates that are sent and received by dynamic routing protocols and how to control the routes that are redistributed into routing protocols. You can control routing updates by using the **passive-interface** command, and by creating and applying distribute lists or route maps. This lesson discusses the use of the **passive-interface** command and distribute lists.

Relevance

Routing updates compete with user data for bandwidth and router resources, yet routing updates are critical because they carry the information that routers need to make sound routing decisions.

To ensure that the network operates efficiently, you must control and tune routing updates. Information about networks must be sent where it is needed, and filtered from where it is not needed. There is no one type of route filter that is appropriate for every situation; therefore, the more techniques that you have at your disposal, the better your chance of having a smooth, well-run network.

Objectives

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

- Describe and configure passive interfaces
- Describe and configure route-filtering techniques using distribute lists
- Explain the implementation of the distribute list route-filtering technique

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge
- Knowledge of routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks

Outline

The outline lists the topics included in this lesson.

Outline

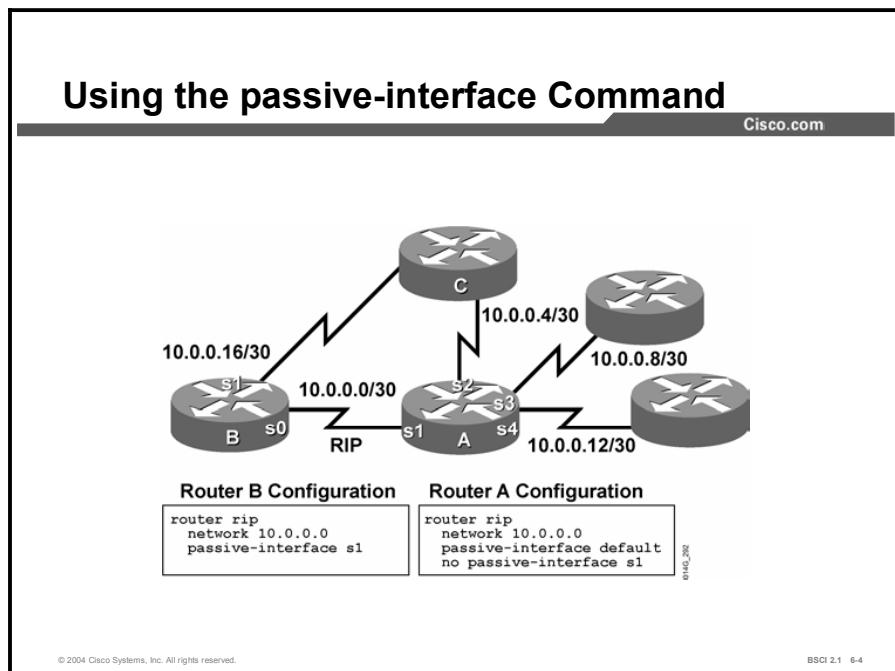
Cisco.com

- **Overview**
- **Passive Interface**
- **Route Filtering**
- **Distribute List**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 6-3

Passive Interface

This topic identifies the **passive-interface** command and its uses.



There are times when you must include an interface in a **network** command, although you do not want that interface to participate in the routing protocol. The **passive-interface** command prevents routing updates for a routing protocol from being sent through a router interface. The **passive-interface** command can set a particular interface, or all router interfaces, to passive. Use the **default** option to set all router interfaces.

With Internet service providers (ISPs) and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the introduction of the passive interface default feature in Cisco IOS Release 12.0, the solution to the numerous interface problems was to configure the routing protocol on all interfaces and manually set the **passive-interface** command on the interfaces where you did not require adjacency.

However, this solution meant entering 200 or more passive-interface statements. You can now solve this configuration scalability problem by using a single **passive-interface default** command to set all interfaces to passive by default. You then enable routing on individual interfaces where you require adjacencies, using the **no passive-interface** command.

When you use the **passive-interface** command with RIP and IGRP, routing updates are not sent out to the specified interface. The router, however, still receives routing updates from that interface.

When you use the **passive-interface** command with EIGRP, hello messages are not sent out to the specified interface. Neighboring router relationships do not form with other routers that are reachable through that interface. If no neighbors are found on an interface, then no other EIGRP traffic is sent.

Using the **passive-interface** command on a router running a link-state routing protocol also prevents the router from establishing neighboring router adjacencies with other routers that are connected to the same link as the one that is specified in the command.

The router does not send hellos to the specified interface. Therefore, you cannot establish neighbor adjacencies because the Hello protocol is used to verify bidirectional communication between routers.

To configure a passive interface, regardless of the routing protocol, use the following procedure:

- Step 1** Select the router and routing protocol that require the passive interface.
- Step 2** Determine the interfaces through which you do not want routing update traffic (or hellos for link-state routing protocols and EIGRP) to be sent.
- Step 3** Configure the router using the **passive-interface** command.

The following table describes the parameters of the **passive-interface** command.

Table 1: The passive-interface Command Parameters

Parameter	Description
type number interface-number	Type of interface and interface number that does not send routing updates or hellos for link-state routing protocols and EIGRP.
default	Sets all interfaces on the router as passive by default.

In the previous figure, routers A and B run RIP, and have a network statement that encompasses all their interfaces. However, you want to run RIP on the link between router A and router B only.

Router A has several interfaces; configure the **passive-interface default** command, and then use the **no passive-interface** command for the one interface from where RIP updates are advertised. Router B has only two interfaces; configure the **passive-interface** command for the one interface that does not participate in RIP routing.

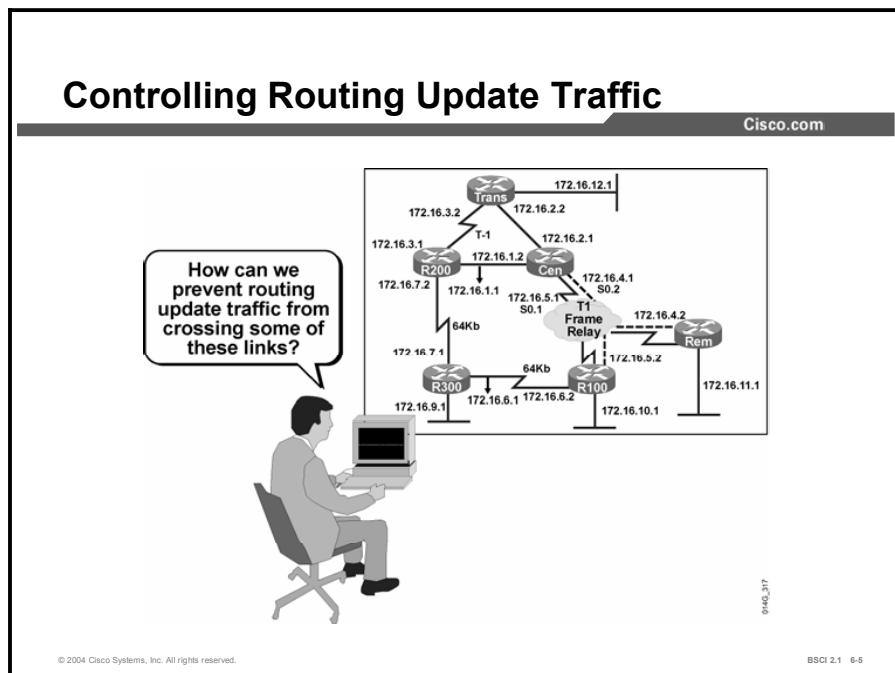
It is important to understand how this configuration affects the information that is exchanged between routers A and B, and router C. Unless you configure another routing protocol and redistribute between it and RIP, router A does not tell router C that it has a way to reach the networks advertised by router B via RIP.

Likewise, router B does not tell router C that it has a way to reach the networks advertised by router A via RIP.

Redundancy is built into this network; however, the three routers are not able to use the redundancy effectively. For example, if the link between router C and router A fails, router C does not know that it has an alternate route through router B.

Route Filtering

This topic describes route filtering techniques using distribute lists.



The passive interface technique prevents all routing updates from being advertised out of an interface. However, in many cases, you do not want to prevent all routing information from being advertised.

You might want to block the advertisement of only certain specific routes. For example, you could use such a solution to prevent routing loops when you are implementing two-way route redistribution with dual redistribution points.

Many companies have prominent redundant paths because of their large networks. When two different routing protocols discover a path to the same destination, the propagation of one of the paths should be filtered.

Some ways to control or prevent dynamic routing updates are as follows:

- **Passive interface:** As previously stated, this feature prevents all routing updates from being sent through an interface. For EIGRP, OSPF, and IS-IS, this method includes Hello protocol packets.
- **Default routes:** This feature instructs the router that if it does not have a route for a given destination, it should send the packet to the default route. Therefore, no dynamic routing updates about the remote destinations are necessary.
- **Static routes:** This feature allows routes to remote destinations to be manually configured in the router. Therefore, no dynamic routing updates about the remote destinations are necessary.

Another way to control routing updates is a technique called a “distribute list.” A distribute list allows the application of an access list to routing updates. Access lists are usually

associated with interfaces and are usually used to control user traffic. However, routers can have many interfaces, and route information can also be obtained through route redistribution, which does not involve an interface at all.

Additionally, access lists do not affect traffic that is originated by the router, so applying one to an interface would have no effect on outgoing routing advertisements. However, when you link an access list to a distribute list, then routing updates can be controlled, no matter what their source is.

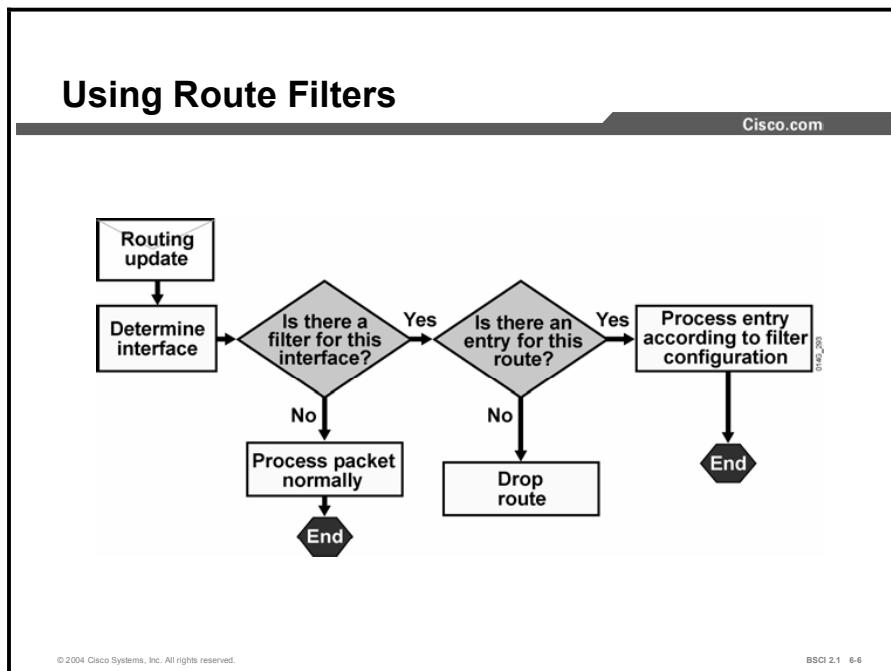
Configure access lists in global configuration mode, and then configure the associated distribute list under the routing protocol. The access list should permit the networks that will be advertised or redistributed and deny the networks that will remain hidden.

The router then applies the access list to routing updates for that protocol. Options in the **distribute-list** command allow updates to be filtered based on three factors:

- Incoming interface
- Outgoing interface
- Redistribution from another routing protocol

Using a distribute list gives the administrator great flexibility in determining just which routes will be permitted and which will be denied.

Example



The figure shows the general process that a router uses when filtering routing updates using a distribute list that is based on the incoming or outgoing interface. The process includes the following steps:

- Step 1** The router receives a routing update or prepares to send an update about one or more networks.
- Step 2** The router looks at the interface involved with the action.
The router checks the interface on which the incoming update has arrived. For an update that must be advertised, the router checks the interface out of which it should be advertised.
- Step 3** The router determines if a filter (distribute list) is associated with the interface.
- Step 4** If a distribute list is not associated with the interface, the packet is processed as normal.
- Step 5** If a distribute list is associated with the interface, the router scans the access list that is referenced by the distribute list for a match for the given routing update.
- Step 6** If there is a match in the access list, the route entry is processed as configured; it is either permitted or denied by the matching access-list statement.
- Step 7** If no match is found in the access list, the “implicit deny any” at the end of the access list causes the route entry to be dropped.

Distribute List

This topic explains the implementation of the distribute list route-filtering technique.

Configuring distribute-list

Cisco.com

For outbound updates:

Router(config-router)#

```
distribute-list {access-list-number | name} out  
[interface-name | routing-process | [autonomous-system  
number]]
```

For inbound updates:

Router(config-router)#

```
Distribute-list {access-list-number | name} in [type  
number]
```

- Use an access list to permit or deny routes.
- An access list can be applied to transmitted, received, or redistributed routing updates.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

You can filter routing update traffic for any protocol by defining an access list and applying it to a specific routing protocol. You use the **distribute-list** command and link it to an access list to complete the filtering of routing update traffic.

A distribute list enables the filtering of routing updates coming into a specific interface from neighboring routers using the same routing protocol, or going out of the interface toward the routers. A distribute list also allows the filtering of routes redistributed from other routing protocols or sources. To configure a distribute list, use the following procedure:

- Step 1** Identify the network addresses that you want to filter and create an access list.
- Step 2** Determine whether you want to filter traffic on an incoming interface, an outgoing interface, or routes being redistributed from another routing source.
- Step 3** Use the **distribute-list out** command to assign the access list to filter outgoing routing updates or to assign it to routes being redistributed into the protocol. The **distribute-list out** command cannot be used with link-state routing protocols for blocking outbound link-state advertisements (LSAs) on an interface.
- Step 4** Use the **distribute-list in** command to assign the access list to filter incoming routing updates coming in through an interface. This command prevents most routing protocols from placing the filtered routes in their database. When this command is used with OSPF, the routes are placed in the database but not the routing table.

This table describes the parameters of the **distribute-list out** command.

Table 2: The distribute-list out Command Parameters

Parameter	Description
<i>access-list-number name</i>	Standard access list number or name.
out	Applies the access list to outgoing routing updates.
<i>interface-name</i>	(Optional) Name of interface out of which updates are filtered.
<i>routing-process</i>	(Optional) Name of the routing process, or the keyword static or connected , that is being redistributed and from which updates are filtered.
<i>autonomous-system-number</i>	(Optional) AS number of the routing process.

To assign the access list to filter incoming routing updates, use the **distribute-list in** command.

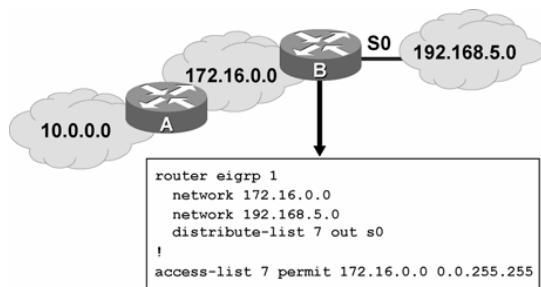
This table describes the parameters of the **distribute-list in** command.

Table 3: The distribute-list in Command Parameters

Parameter	Description
<i>access-list-number name</i>	Standard access list number or name.
in	Applies the access list to incoming routing updates.
<i>interface-type interface-number</i>	(Optional) Interface type and number from which updates are filtered.

Filtering Routing Updates with a Distribute List

Cisco.com



- Hides network 10.0.0.0 using interface filtering

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-8

The following table describes some of the commands shown in the figure.

Table 4: The distribute-list Configuration Commands

Command	Description
distribute-list 7 out s0	Applies access list 7 as a route filter on EIGRP routing updates sent out interface serial 0.
access-list 7 permit 172.16.0.0 0.0.255.255	Configures a standard access list to permit routing information regarding only the 172.16.0.0 network.

The **distribute-list 7 out s0** command applies access list 7 to routing updates sent out from interface serial 0 to other routers running this routing protocol. This access list permits routing information about only network 172.16.0.0.

The implicit deny any at the end of the access list prevents routing updates regarding any other networks from being advertised. As a result, network 10.0.0.0 is hidden from the rest of the network.

Controlling Redistribution with Distribute Lists

Cisco.com



Router B Configuration:

```
router ospf 1
network 10.0.0.8 0.0.0.3 area 0
redistribute rip subnets
distribute-list 2 out rip

router rip
network 10.0.0.0
version 2
passive-interface s3
redistribute ospf 1 metric 5
distribute-list 3 out ospf 1

access-list 2 deny 10.3.0.0 0.0.0.255.255
access-list 2 permit any
access-list 3 permit 10.9.0.0
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-9

Using a distribute list with redistribution helps prevent route feedback, which also helps prevent routing loops. Route feedback occurs when routes originally learned from one routing protocol get redistributed back into that protocol.

As shown in the figure, two-way redistribution is completed between RIP and OSPF. Networks 10.1.0.0 to 10.3.0.0 redistribute from RIP into OSPF. Route feedback could occur if another redistribution point was configured in the future and OSPF then redistributed those same networks back into RIP.

Although there is a single redistribution point, the figure shows an example of configuring distribute lists to prevent route feedback. Access list 2 denies the original OSPF routes and permits all others. The distribute list configured under OSPF refers to this access list.

The result is that networks 10.8.0.0 to 10.11.0.0, originated by OSPF, are not redistributed back into OSPF from RIP. Redistribution into RIP from OSPF is filtered with access list 3, but with a more restrictive filter that permits only one route, 10.9.0.0.

A distribute list hides network information, which could be considered a drawback in some circumstances. In a network with redundant paths, the goal of using a distribute list may be to prevent routing loops. The distribute list permits routing updates that enable only the desired paths to be advertised; therefore, other routers in the network do not know about other ways to reach the filtered networks.

If the primary path goes down, the backup paths are not used because the rest of the network does not know that they exist. When redundant paths exist, you should use other techniques, such as manipulating administrative distance or the metric, instead of distribute lists, to enable the use of an alternate path (with a worse administrative distance or metric) when the primary path goes down.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The passive-interface command has two options:**
 - Specify an interface
 - Set all interfaces on the router as passive by using the default option
- **Route filtering can be applied to route distribution to prevent route feedback when you are performing two-way route redistribution with multiple redistribution points.**
- **Routing update traffic can be filtered for any protocol by defining an access list and applying it to a specific routing protocol using the distribute-list command and linking it to an access list.**

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 two actions does the **passive-interface** command prevent? (Choose two.)
- A) prevents routing updates from being sent out from an interface, but not from being received on an interface
 - B) prevents routing updates from being sent out from an interface, and also from being received on an interface
 - C) prevents link-state protocols and EIGRP from sending hellos out of the interface
 - D) prevents the exchange of routing updates only, not hellos
- Q2) Configuring a distribute list allows the filtering of routes based on which three factors? (Choose three.)
- A) the routing protocol originating the advertisement
 - B) the incoming interface of the advertisement
 - C) the outgoing interface of the advertisement
 - D) the administrative distance of the route
- Q3) Which command do you use to configure filtering of specific routes in the routing update traffic that a routing protocol sends out from an interface?
- A) **passive-interface**
 - B) **distribute-list out**
 - C) **distribute-list in**
 - D) **redistribute <protocol>**

Quiz Answer Key

Q1) A, C

Relates to: Passive Interface

Q2) A, B, C

Relates to: Route Filtering

Q3) B

Relates to: Distribute List

Using Route Maps to Control Routing Updates

Overview

Route maps are used for a variety of purposes. This lesson explores the use of route maps as a tool to filter and manipulate routing updates. All the IP routing protocols can use route maps for redistribution filtering. This lesson discusses examples using RIP, OSPF, and EIGRP.

Relevance

Using route maps for the manipulation and control of routing protocol updates is the technique preferred by Cisco Systems. It is important that network operators understand and use route maps when redistributing routes between routing protocols.

Objectives

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

- Describe the operation of a route map
- Use **route-map** commands
- Explain how route maps are implemented with route redistribution

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge
- Knowledge of routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) networks

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Route Map Operation**
- **Route-map Commands**
- **Route Maps with Redistribution**
- **Summary**
- **Quiz**

Route Map Operation

Route maps are powerful and flexible configuration tools. This topic defines the concept of route maps and describes their operation.

Route Maps

Cisco.com

Route maps are similar to a scripting language for the following reasons:

- **They work like a more sophisticated access list.**
 - Top-down processing
 - Once there is a match, leave the route map
- **Lines are sequence-numbered for easier editing.**
 - Insertion of lines
 - Deletion of lines
- **Route maps are named rather than numbered for easier documentation.**
- **Match criteria and set criteria can be used, similar to the “if, then” logic in a scripting language.**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 6-4

Route maps are complex access lists that allow conditions to be tested against a packet or route using the **match** commands. If the conditions match, then actions can be taken to modify attributes of the packet or route. These actions are specified by the **set** commands.

A collection of route map statements that have the same route map name is considered one route map. Within a route map, each route map statement is numbered and can be edited individually.

The statements in a route map are analogous to the lines of an access list. Specifying the match conditions in a route map is similar to specifying the source and destination addresses and masks in an access list.

One major difference between route maps and access lists is that route maps can use the **set** commands to modify the packet or route.

Route Map Applications

Cisco.com

Following are the common uses of route maps:

- **Redistribution route filtering:** a more sophisticated alternative to distribute lists
- **Policy-based routing:** the ability to determine routing policy based on criteria other than the destination network
- **NAT:** defines pools of public and private address space that are used in translation
- **BGP policy implementation:** the primary tool for defining BGP routing policies

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-6

Network administrators use the route map tool for a variety of purposes. Several of the more common applications for route maps are as follows:

- **Route filtering during redistribution:** Redistribution nearly always requires some amount of route filtering. Whereas distribute lists can be used for this purpose, route maps offer an added benefit of manipulating routing metrics through the use of the **set** commands.
- **Policy-based routing (PBR):** Route maps can be used to match source and destination addresses, protocol types, and end-user applications. Once a match occurs, a **set** command describes the interface or next-hop address to which the packet should be sent. PBR allows the operator to define routing policy other than basic destination-based routing using the routing table.
- **Network Address Translation (NAT):** Route maps can better control which private addresses are translated to public addresses. Using a route map with NAT also provides more detailed **show** commands that describe the address translation process.
- **Border Gateway Protocol (BGP):** Route maps are the primary tools for implementing BGP policy. Network administrators assign route maps to specific BGP sessions (neighbors) to control which routes are allowed to flow into and out of the BGP process. In addition to filtering, route maps provide sophisticated manipulation of BGP path attributes.

Route Map Operation

Cisco.com

- A list of statements composes a route map.
- The list is processed top-down like an access list.
- The first match found for a route is applied.
- The sequence number is used for inserting or deleting specific route map statements.

```
route-map my_bgp permit 10
  :: :: ::
  { match statements }
  :: :: ::
  { set statements }
route-map my_bgp deny 20
  :: :: ::
  :: :: ::
route-map my_bgp permit 30
  :: :: ::
  :: :: ::
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-6

Route maps operate in a manner similar to access lists. When determining which routes will be redistributed from one protocol to the next, the router checks each route against the route map, beginning with the top line.

Each line is sequence-numbered, both for top-down processing purposes and for editing purposes. Lines can be added or removed from a route map as changes are required.

Each line has a permit or deny statement. If a route is matched in the matching statements and the line statement is “permit,” then the router sets the metrics or other defined conditions and permits the redistribution of that route. The route map stops processing at the first match.

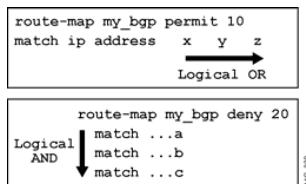
If the packet is matched and the route map line is “deny,” then the router stops at the matched line in the map and does not redistribute that route. Routes are filtered by this method.

Routes are checked from line to line looking for a match. If there is no match, and the bottom of the route map is reached, then the router denies the route from being redistributed. There is always an implicit deny at the end of a route map.

Route Map Operation (Cont.)

Cisco.com

- The match statement may contain multiple references.
- Multiple match criteria in the same line use a logical OR.
- At least one reference must permit the route for it to be a candidate for redistribution.



- Each vertical match uses a logical AND.
- All match statements must permit the route for it to remain a candidate for redistribution.
- Route-map permit or deny determines if the candidate will be redistributed.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

Match statements in a route map can be complex. Multiple match criteria in the same line are processed with OR logic. Separate match criteria can also be applied vertically under a route map line. In this case, each match uses AND logic.

A route map may consist of multiple route map statements. The statements are processed top-down, like an access list. The first match found for a route is applied. The sequence number is used for inserting or deleting specific route map statements in a specific place in the route map.

The **match** route map configuration commands define the conditions to be checked. The **set** route map configuration commands define the actions that you should follow if there is a match.

The single-match statement may contain multiple conditions. At least one condition in the match statement must be true to consider the statement a match (logical OR). A route map statement may contain multiple match statements. All match statements in the route map statement must be true to consider the route map statement a match (logical AND).

The sequence number specifies the order in which conditions are checked. For example, if there are two statements in a route map named MYMAP, one with sequence 10 and the other with sequence 20, sequence 10 is checked first. If the match conditions in sequence 10 are not met, then sequence 20 is checked.

Like an access list, there is an implicit deny any at the end of a route map. The consequences of this deny depend on how the route map is used.

Example

The route map in the previous figure is interpreted as follows:

- If the route matches X or Y or Z, then permit

Otherwise,

- If the route matches A and B and C, then deny

route-map Commands

This topic defines the basic **route-map** command syntax that is used during configuration.

Route-map Commands

Cisco.com

```
router(config-router)#
  redistribute protocol [process id] route-map map-tag
```

- Allows for detailed control of routes being redistributed into a routing protocol

```
router(config)#
  route-map map-tag [permit | deny] [sequence-number]
```

- Defines the route map conditions

```
router(config-route-map)#
  match {conditions}
```

- Defines the conditions to match

```
router(config-route-map)#
  set {actions}
```

- Defines the action to be taken on a match

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-8

The **route-map** command is used to define the conditions for route filtering and redistribution. The following table describes the parameters of the **route-map** command.

Table 1: The route-map Command Parameters

Parameter	Description
<i>map-tag</i>	The name of the route map.
permit deny	The action to be taken if the route map match conditions are met <ul style="list-style-type: none">■ permit = permit the matched route to be redistributed■ deny = deny the matched route from being redistributed
<i>sequence-number</i>	Sequence number that indicates the position that a new route map statement will have in the list of route map statements already configured with the same route map name.

When used for redistribution filtering, a route map is applied to the route redistribution process by adding the **route-map** command and *map-tag* to the end of the **redistribute protocol** command.

A route map may consist of multiple route map statements. The statements are processed top-down, like an access list. The first match found for a route is applied. The sequence number is used for inserting or deleting specific route map statements in a specific place in the route map.

The match Command

Cisco.com

```
router(config-route-map)#
```

- The match commands specify criteria to be matched.
- The associated route map statement permits or denies the matching routes.

```
Match {options}
options :
ip address ip-access-list
ip route-source ip-access-list
ip next-hop ip-address-list
interface type number
metric metric-value
route-type [external | internal | level-1 | level-2 | local]
...
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-9

The **match** command is applied under a route map line. The table lists the variety of match criteria that can be defined.

Table 2: The match Commands

Command	Description
match community	Matches a BGP community.
match interface	Distributes any routes that have the next hop out of one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
match ip next-hop	Redistributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address that is specified by the access lists.
match length	Bases policy routing on the level-3 length of a packet.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.

The table presents a general list of match criteria; some are used for BGP policy, some for PBR, and some for redistribution filtering.

The set Command

Cisco.com

```
router(config-route-map) #
```

- The **set** commands modify matching routes.
- The command modifies parameters in redistributed routes.

```
set {options}
  options :
    metric metric-value
    metric-type [type-1 | type-2 | internal | external]
    level [level-1 | level-2 | stub-area | backbone]
    ip next-hop next-hop-address
```

```
bgp specific options :
  origin bgp-origin-code
  weight bgp-weight
  local-preference bgp-path-attributes
  automatic-tag
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-10

The **set** commands are used under a route map line to change or add characteristics, such as metrics, to any routes that have met a match criterion. Each **set** option is described in the following table.

Table 3: The set Commands

Command	Description
set as-path	Modifies an AS path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set level	Indicates where to import routes for IS-IS and OSPF.
set local-preference	Specifies a local preference value for the AS path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

Not all the **set** options that are listed here are used for redistribution purposes. The table includes options for BGP and PBR.

Route Maps with Redistribution

This topic provides an example to explain how route maps can be used to filter routes during redistribution.

Route Maps and Redistribution Commands

Cisco.com

```
Router(config)# router ospf 10
Router(config-router)# redistribute rip route-map redis-rip
```

- Routes matching either access list 23 or 29 are redistributed with an OSPF cost of 500, external type 1.
- Routes permitted by access list 37 are not redistributed.
- All other routes are redistributed with an OSPF cost metric of 5000, external type 2.

```
Router(config)#
route-map redis-rip permit 10
match ip address 23 29
set metric 500
set metric-type type-1

route-map redis-rip deny 20
match ip address 37

route-map redis-rip permit 30
set metric 5000
set metric-type type-2
```

```
Router(config)#
access-list 23 permit 10.1.0.0 0.0.255.255
access-list 29 permit 172.16.1.0 0.0.0.255
access-list 37 permit 10.0.0.0 0.255.255.255
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-11

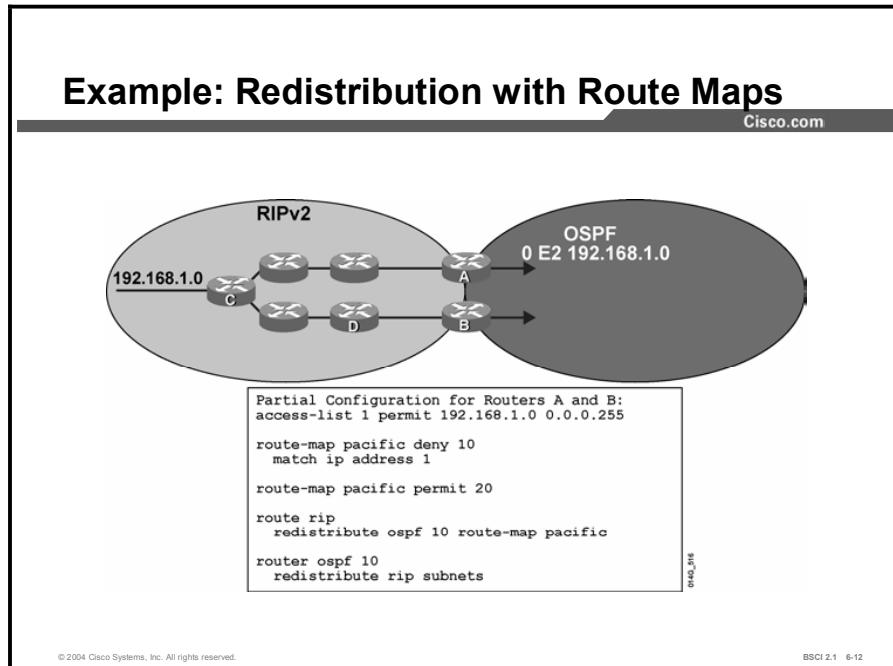
In this example, RIPv1 is being redistributed into OSPF 10. A route map called “redis-rip” has been attached to the **redistribute rip** command.

Sequence number 10 of the route map is looking for an IP address match in access list 23 or access list 29. If a match is found, then the router redistributes the route into OSPF with a cost metric of 500 and sets the new OSPF route to external type 1.

If there is no match to line 10, move to line 20. If there is a match in access list 37, then do not let that route redistribute into OSPF because sequence number 20 is a deny.

If there is no match to sequence number 20, move to 30. Because 30 is a permit and there is no match criterion, all remaining routes are redistributed into OSPF with a cost metric of 5000 and an external metric of type 2.

Example



There is a possibility of routing feedback causing suboptimal routing or a routing loop when routes are redistributed at more than one router. In this example, mutual redistribution (redistribution in both directions) is configured on routers A and B. To prevent redistribution feedback loops, route maps are configured on both routers.

The potential for routing feedback becomes apparent if you follow the advertisements for a specific network when route maps have not been configured. For example, RIPv2 on router C advertises network 192.168.1.0. Router A (and B) redistribute the network into OSPF.

OSPF then advertises the route to its neighbor OSPF routers as an OSPF external route. The route filters through the OSPF AS and eventually makes its way back to the other edge router. Router B (or A) then redistributes 192.168.1.0 from OSPF back into the original RIPv2 network. This condition is known as a route feedback loop.

To prevent the routing feedback loop, a route map has been applied to routers A and B. The route map statement with sequence number 10 refers to an access list that matches the original RIP network. This statement is a deny statement, so those routes will be denied from redistribution back into RIP.

The router will then apply sequence number 20, which is an empty permit statement. This statement matches all routes, so all other routes will be redistributed into RIP.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **A route map is a complex tool used for manipulating and filtering routes.**
- **Route maps work similarly to access lists, but offer better editing features and complex match and set commands for route manipulation.**
- **When used for redistribution, route maps match routes. These routes are either permitted to redistribute or denied. If permitted, the metric value can be specified as the route is redistributed into the new protocol.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-13

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 6-1: Configuring Basic Redistribution

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 three uses for route maps? (Choose three.)
- A) policy-based routing
 - B) setting BGP policy
 - C) managing password configurations
 - D) redistribution filtering
- Q2) Which statement does not describe route map operation?
- A) Routes maps use a top-down processing scheme.
 - B) Route maps use match and set logic to match a metric and then set which route is redistributed.
 - C) Route maps are line-numbered for easier editing.
 - D) Route maps use an implicit deny at the bottom of the map, just like access lists.
- Q3) When you are configuring a route map, you must define a map tag.
How is a map tag used?
- A) to tag a route in a **set** command
 - B) to match on a tagged route in a **match** command
 - C) to deny routes from being redistributed
 - D) to give a name to the route map
- Q4) Define each variable listed as “match,” “set,” or “match and set” if it does both.
- A) **IP address** _____
 - B) **tag** _____
 - C) **metric** _____
 - D) **interface** _____
 - E) **route-source** _____
- Q5) What are the commands that you use to apply a route map called TEST when filtering traffic from OSPF 10 into EIGRP 20?

Quiz Answer Key

Q1) A, B, D

Relates to: Route Map Operation

Q2) B

Relates to: Route Map Operation

Q3) D

Relates to: Route Map Commands

Q4) A - match, B - match and set, C - match and set, D - match and set, E - match and set

Relates to: Route Map Commands

Q5) **router eigrp 20**

redistribute ospf 10 route-map TEST

Relates to: Route Maps with Redistribution

Using Administrative Distance to Influence the Route Selection Process

Overview

Controlling administrative distance is an important way to mark preference in route selection. Changing the default administrative distance should be done carefully and with consideration for the specific requirements of the network.

Relevance

Route selection is sometimes confusing because of redistribution. The redistribution point is a demarcation between two different methods of resolving the best path. As a result, important information is lost going through redistribution, namely the relative metrics of routes. One approach for correcting wayward choices is by controlling the administrative distance so that route selection is unambiguous. This approach does not always guarantee the best route selection, only a consistent choice for route selection.

Objectives

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

- List the benefits of manipulating administrative distance
- Use the **distance** commands to modify the default administrative distance of certain routes to influence the route selection process
- Describe the impact of administrative distance changes on routing tables

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Purpose of Administrative Distance**
- **Commands for Changing Administrative Distance**
- **Examples of Redistribution Using Administrative Distance**
- **Summary**
- **Quiz**

Purpose of Administrative Distance

This topic describes how administrative distance ranks sources of routing information by trustworthiness, allowing a comparison of routes even when routing protocols use incomparable metrics.

Administrative Distance

- Administrative distance is a way of ranking the trustworthiness of routing information. Administrative distance is expressed as an integer, from 0 to 255. Lower administrative distance is more trustworthy.
- For R1 to R6:
 - RIP (administrative distance 120) would choose R1-R4-R6.
 - IS-IS (administrative distance 115) would choose R1-R4-R6.
 - OSPF (administrative distance 110) would choose R1-R2-R3-R5-R6.
 - EIGRP (administrative distance 90) would choose R1-R2-R3-R5-R6.

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 6-4

Multiple sources of routing information may be active at the same time, including static routes and routing protocols that use various methods of operation and metrics. Routers must identify which routing information source is trustworthy and reliable, given several sources of information that supply ambiguous next-hop information for a particular prefix.

Administrative distance is a way to rank sources of routing information with lower values, which indicate greater believability.

Example

In the figure, for the best path from R1 to R6, the following route choices are made if all four routing protocols are active on all the routers:

- Routing Information Protocol (RIP) (administrative distance 120) chooses R1 to R4 to R6 based on hop count (two hops versus four hops the other way).
- Intermediate System-to-Intermediate System (IS-IS) (administrative distance 115), using the default metric of 10 for each interface, also chooses R1 to R4 to R6 based on a metric of 20 versus 40 the other way.

Modifying the IS-IS metrics to portray a more accurate view of the network is possible. IS-IS is more trustworthy than RIP because it is a link-state routing protocol with fast convergence, so its routing information is more complete and up to date.

- Open Shortest Path First (OSPF) (administrative distance 110) calculates the default metric as 100 Mbps divided by the interface bandwidth (BW), where BW is the speed of each link.
The path R1 to R4 to R6 default metric is $(100 \text{ Mbps} / 64 \text{ kbps}) + (100 \text{ Mbps} / 1.544 \text{ Mbps}) = 1562 + 64$, or 1626. The R1 to R2 to R3 to R5 to R6 path default metric is $1544 + 1544 + 1544 + 1544 = 6176$. Therefore, OSPF chooses the R1 to R2 to R3 to R5 to R6 path.

Although OSPF and IS-IS are both link-state routing protocols that converge quickly, OSPF is more trustworthy than IS-IS because OSPF bases its default metric on bandwidth and is therefore more likely to pick the best path.

- Enhanced Interior Gateway Routing Protocol (EIGRP) (administrative distance 90) calculates the default metric as $(100,000,000 / \text{BW}) + \text{delay}$, where BW is the speed of the slowest link in the path and delay is cumulative across the path.

Assuming a uniform link delay of 100, the R1 to R4 to R6 default metric is $(10^8 / 64) + 200 = 1,562,700$, and R1 to R2 to R3 to R5 to R6 default metric is $(10^8 / 1544) + 400 = 65,166$.

Therefore, EIGRP chooses R1 to R2 to R3 to R5 to R6. Although EIGRP and OSPF routing protocols both converge quickly and consider bandwidth,

EIGRP is more trustworthy than OSPF because EIGRP takes more information into account in its calculation. Because EIGRP has the lowest administrative distance of the four protocols, only the EIGRP path is put into the routing table.

Commands for Changing Administrative Distance

This topic identifies how administrative distance may be modified globally on the router for a particular routing protocol or specifically for certain routes.

Modifying Administrative Distance

Cisco.com

```
Router (config-router)#
  distance weight [address wildcard-mask [access-list-
    number | name]]
```

- Used for all protocols except EIGRP and BGP redistribution

```
Router (config-router)#
  distance eigrp internal-distance external-distance
```

- Used for EIGRP redistribution

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 6-5

In some cases, a router selects a suboptimal path if it believes a routing protocol with a better administrative distance, even though it is actually a routing protocol with a worse route.

Assigning an undesired routing protocol a larger administrative distance ensures that routers select routes from the desired routing protocol. The figure illustrates the commands for changing the default administrative distance.

The **distance** command changes the default administrative distance for all protocols except EIGRP and BGP. The following table explains each field in the **distance** command.

Table 1: The distance Command Parameters

Parameter	Description
<i>weight</i>	The administrative distance. An integer from 1 to 255. Routes with a distance of 255 are not installed in the routing table. A value of 0 is reserved for directly connected networks.
<i>address</i>	(Optional) The IP address filters networks according to the IP address of the router supplying the routing information.
<i>wildcard-mask</i>	(Optional) The wildcard mask for an IP address. A bit set to 1 in the mask argument instructs the software to ignore the corresponding bit in the address value. Use an address/mask of 0.0.0.0 255.255.255.255 to match any IP address (any source router supplying the routing information).
<i>access-list-number name</i>	(Optional) The number or name of the standard access list to apply to incoming routing updates. It allows filtering of the advertised networks.

For EIGRP, use the **distance eigrp** command. EIGRP assigns different administrative distance values to routes learned natively through EIGRP and to routes redistributed in from other sources. By default, natively learned routes have an administrative distance of 90, but external routes have an administrative distance of 170.

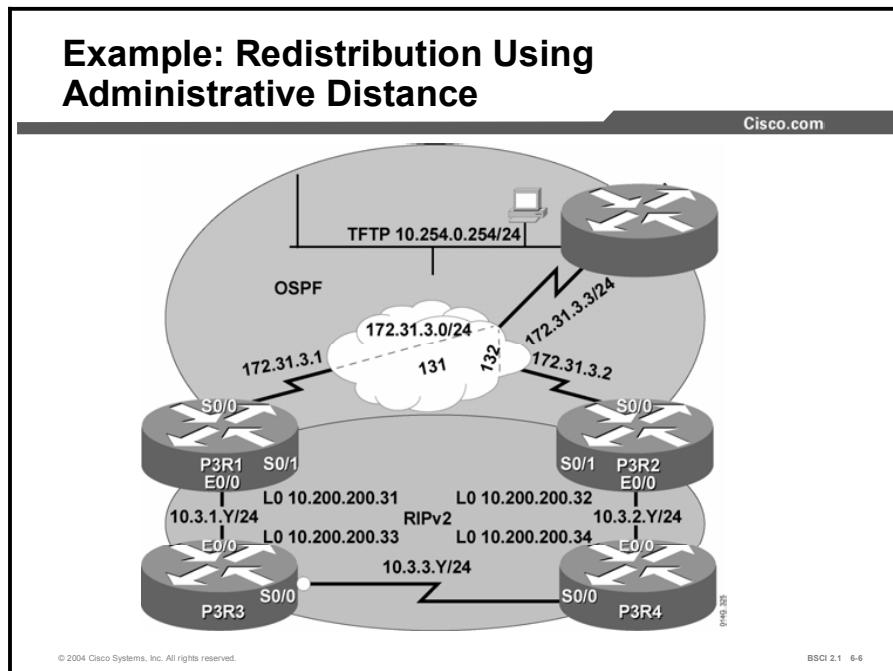
Table 2: The distance eigrp Command Parameters

Parameter	Description
<i>external-distance</i>	The administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a neighbor external to the AS.
<i>internal-distance</i>	The administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the AS.

For BGP, use the **distance bgp** command. BGP assigns different administrative distance values to routes learned through Internal Border Gateway Protocol (IBGP) and routes learned through External Border Gateway Protocol (EBGP).

Examples of Redistribution Using Administrative Distance

This topic describes a network using multiple routing protocols. There are a number of ways to correct path selection problems in a redistribution environment. The purpose of this example is to show how a problem can occur, where it appears, and one possible way of resolving it.



The figure illustrates a network with RIP and OSPF routing domains. Recall that OSPF is more believable than RIP because it has an administrative distance of 110 and RIP has an administrative distance of 120.

If, for example, the boundary router (P3R1 or P3R2) learns about network 10.3.3.0 via RIPv2 and also via OSPF, the OSPF route is used and inserted into the routing table because OSPF has a lower administrative distance than RIPv2, even though the path via OSPF might be the longer (worse) path.

Example: Redistribution Using Administrative Distance (Cont.)

Cisco.com

Router P3R1

```
router ospf 1
 redistribute rip metric 10000 metric-type 1 subnets
 network 172.31.0.0 0.0.255.255 area 0
!
router rip
 version 2
 redistribute ospf 1 metric 5
 network 10.0.0.0
 no auto-summary
```

Router P3R2

```
router ospf 1
 redistribute rip metric 10000 metric-type 1 subnets
 network 172.31.3.2 0.0.0.0 area 0
!
router rip
 version 2
 redistribute ospf 1 metric 5
 network 10.0.0.0
 no auto-summary
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

The figure illustrates the configurations for the P3R1 and P3R2 routers. These configurations redistribute RIP into OSPF and OSPF into RIP on both routers.

The redistribution into OSPF sets a default OSPF metric of 10000 to make these routes less preferred than native OSPF routes and protect against route feedback. The redistribute statement also sets the metric type to E1, so that the route metrics continue to accrue, and the router redistributes subnet information.

The redistribution into RIP sets a default RIP metric of 5 to also protect against route feedback.

Example: Redistribution Using Administrative Distance (Cont.)

Cisco.com

With OSPF and RIP running:



```
P3R2#show ip route
<Output Omitted>
Gateway of last resort is not set
      172.31.0.0/24 is subnetted, 7 subnets
o   172.31.55.0 [110/2343] via 172.31.3.3, 00:09:46, Serial0/0
o   172.31.3.0 is directly connected, Serial0/0
o   172.31.2.0 [110/1562] via 172.31.3.3, 00:09:46, Serial0/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
o E1  10.3.1.0/24 [110/10781] via 172.31.3.1, 00:09:47, Serial0/0
o E1  10.3.3.0/24 [110/10781] via 172.31.3.1, 00:04:51, Serial0/0
C     10.3.2.0/24 is directly connected, Ethernet0/0
o E1  10.200.200.31/32 [110/10781] via 172.31.3.1, 00:09:48, Serial0/0
o E1  10.200.200.34/32 [110/10781] via 172.31.3.1, 00:04:52, Serial0/0
C     10.200.200.32/32 is directly connected, Loopback0
o E1  10.200.200.33/32 [110/10781] via 172.31.3.1, 00:04:52, Serial0/0
o E2  10.254.0.0/24 [110/50] via 172.31.3.3, 00:09:48, Serial0/0
```

• P3R2 includes suboptimal paths, loops

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-8

This figure displays the routing table on the P3R2 router after redistribution has occurred. The P3R2 router learned RIP and OSPF routes but lists only OSPF routes in the routing table.

The first edge router to set up redistribution has a normal routing table and retains the RIP routes. The second edge router chooses the OSPF routes over its RIP routes. The paths to the internal RIP routes are shown as going through the core because of the dual mutual redistribution points.

OSPF is informed about the RIP routes via redistribution. OSPF then advertises the RIP routes via OSPF routes to its neighboring router. The neighbor router is also informed about the same routes via RIP; however, OSPF has a better administrative distance than RIP so the RIP routes are not put into the routing table.

OSPF was configured on the P3R1 router first, and P3R2 then received information about the internal (native RIP) routes from both OSPF and RIP. It prefers the OSPF routes because OSPF has a lower administrative distance; therefore, none of the RIP routes appear in the table.

Refer back to the topology diagram to trace some of the routes. The redistribution has resulted in suboptimal paths to many of the networks.

For instance, 10.200.200.34 is a loopback interface on router P3R4. P3R4 is directly attached to P3R2; however, the OSPF path to that loopback interface goes through P3R1, then P3R3, then P3R4 before it reaches its destination. The OSPF path taken is actually a longer (worse) path than the more direct RIP path.

Example: Redistribution Using Administrative Distance (Cont.)

Cisco.com

```
hostname P3R1
!
router ospf 1
 redistribute rip metric 10000 metric-type 1
 subnets
 network 172.31.0.0 0.0.255.255 area 0
 distance 125 0.0.0.0 255.255.255.255 64
!
router rip
 version 2
 redistribute ospf 1 metric 5
 network 10.0.0.0
 no auto-summary
!
access-list 64 permit 10.3.1.0
access-list 64 permit 10.3.3.0
access-list 64 permit 10.3.2.0
access-list 64 permit 10.200.200.31
access-list 64 permit 10.200.200.34
access-list 64 permit 10.200.200.32
access-list 64 permit 10.200.200.33
```

```
hostname P3R2
!
router ospf 1
 redistribute rip metric 10000 metric-type 1
 subnets
 network 172.31.3.2 0.0.0.0 area 0
 distance 125 0.0.0.0 255.255.255.255 64
!
router rip
 version 2
 redistribute ospf 1 metric 5
 network 10.0.0.0
 no auto-summary
!
access-list 64 permit 10.3.1.0
access-list 64 permit 10.3.3.0
access-list 64 permit 10.3.2.0
access-list 64 permit 10.200.200.31
access-list 64 permit 10.200.200.34
access-list 64 permit 10.200.200.32
access-list 64 permit 10.200.200.33
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-9

One of the boundary routers (P3R2 in this example) selected the poor paths because OSPF has a better administrative distance than RIP. You can change the administrative distance of the redistributed RIP routes to ensure that the boundary routers select the native RIP routes, as illustrated in the figure.

The **distance** command modifies the administrative distance of the OSPF routes to the networks that match access list 64. The table describes some of the command parameters used in the example.

Table 3: The distance Command Parameters

Parameter	Description
125	Defines the administrative distance that specified routes will be assigned.
0.0.0.0 255.255.255.255	Defines the source address of the router supplying the routing information—in this case any router.
64	Defines the access list to be used to filter incoming routing updates to determine which will have their administrative distance changed.

Access list 64 is used to match all the native RIP routes. The **access-list 64 permit 10.3.1.0** command configures a standard access list to permit the 10.3.1.0 network. Other similar access-list statements permit the other internal native RIP networks. The following table describes some of the command parameters used in the example.

Table 4: The access-list Parameters

Parameter	Description
64	The access list number.
permit	Allows all networks that match the address to be permitted, in this case to have their administrative distance changed.
10.3.1.0	A network to be permitted, in this case, to have its administrative distance changed.

In the preceding figure, both of the redistributing routers are configured to assign an administrative distance of 125 to OSPF routes that are advertised for the networks that are listed in access list 64.

Access list 64 has permit statements for the internal native RIP networks of 10.3.1.0, 10.3.2.0, and 10.3.3.0, and the loopback networks of 10.200.200.31, 10.200.200.32, 10.200.200.33, and 10.200.200.34.

Therefore, when either one of the redistributing routers learns about these networks from RIP, it selects the routes learned from RIP (with a lower administrative distance of 120) over the same routes learned from OSPF (with an administrative distance of 125), and puts only the RIP routes in the routing table.

Note that the **distance** command is part of the OSPF routing process configuration because the administrative distance should be changed for these routes when they are advertised by OSPF, not by RIP.

You need to configure the **distance** command on both redistributing routers because either one can have suboptimal routes, depending on which redistributing router sends the OSPF updates about the RIP networks to the other redistributing router first.

Example: Redistribution Using Administrative Distance (Cont.)

Cisco.com

With OSPF changing administrative distance:



```
Gateway of last resort is not set
      172.31.0.0/16 is variably subnetted, 8 subnets, 2 masks
o   172.31.55.4/32 [110/781] via 172.31.33.4, 00:00:01, Serial0/0
C   172.31.33.0/24 is directly connected, Serial0/0
o   172.31.33.1/32 [110/1562] via 172.31.33.4, 00:00:01, Serial0/0
o   172.31.33.4/32 [110/781] via 172.31.33.4, 00:00:01, Serial0/0
o   172.31.44.4/32 [110/781] via 172.31.33.4, 00:00:01, Serial0/0
o   172.31.22.4/32 [110/781] via 172.31.33.4, 00:00:01, Serial0/0
o   172.31.11.4/32 [110/781] via 172.31.33.4, 00:00:03, Serial0/0
o   172.31.66.4/32 [110/781] via 172.31.33.4, 00:00:03, Serial0/0
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
R   10.3.1.0/24 [120/2] via 10.3.2.4, 00:00:03, Ethernet0/0
R   10.3.3.0/24 [120/1] via 10.3.2.4, 00:00:03, Ethernet0/0
C   10.3.2.0/24 is directly connected, Ethernet0/0
R   10.200.200.31/32 [120/3] via 10.3.2.4, 00:00:04, Ethernet0/0
R   10.200.200.34/32 [120/1] via 10.3.2.4, 00:00:04, Ethernet0/0
C   10.200.200.32/32 is directly connected, Loopback0
R   10.200.200.33/32 [120/2] via 10.3.2.4, 00:00:04, Ethernet0/0
o E2  10.254.0.0/24 [110/50] via 172.31.33.4, 00:00:04, Serial0/0
```

- Router P3R2 prefers RIP routes

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-10

The output shows that router P3R2 now retains the more direct paths to the internal networks by learning them from RIP.

However, some routing information is lost with this configuration. For example, depending on the actual bandwidths, the OSPF path may have been better for the 10.3.2.0 network. It may have made sense not to include 10.3.2.0 in the access list.

This example illustrates the importance of knowing your network prior to implementing redistribution, and closely examining which routes that the routers are selecting after redistribution is enabled. Pay particular attention to routers that can select from a number of possible redundant paths to a network, because they are more likely to select suboptimal paths.

The most important feature of using administrative distance to control route preference is that no path information is lost; the OSPF information is still in the OSPF database. If the primary path is lost, the OSPF path can reassert itself, and the router will maintain connectivity with those networks.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Administrative distance allows comparison of routes even when routing protocols use incomparable metrics by ranking sources of routing information by trustworthiness, where lower values indicate greater reliability.**
- **Administrative distance can be modified globally on the router for a particular routing protocol or specifically for certain routes.**
- **There are a number of ways to correct path selection problems in a redistribution environment.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-11

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 6-2: Tuning Basic Redistribution with Cisco IOS Tools

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 does administrative distance rank?
- A) metrics
 - B) sources of routing information
 - C) router reliability
 - D) best paths
- Q2) Which two of the following describe the *weight* variable in the **distance** command?
(Choose two.)
- A) indicates the route metric
 - B) is in the range of 1 to 255
 - C) indicates preference of a routing source
 - D) is multiplied by the metric to get a total administrative metric
- Q3) The **distance** command configurations apply to _____.
_____.
- A) all routers in the routing domain (communicated)
 - B) the router on which it is applied (not communicated)
 - C) all link-state routers (communicated in the link-state advertisement)
 - D) all IGRP and EIGRP routers (communicated through these distance vector routing protocols)

Quiz Answer Key

Q1) B

Relates to: Purpose of Administrative Distance

Q2) B, C

Relates to: Commands for Changing Administrative Distance

Q3) B

Relates to: Examples of Redistribution Using Administrative Distance

Policy-Based Routing

Overview

In the high-performance internetworks of today, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns.

Where administrative issues dictate that traffic be routed through specific paths, policy-based routing (PBR) can provide the solution. Using PBR allows customers to implement policies that selectively cause packets to take different paths.

Relevance

PBR provides network designers greater flexibility in determining traffic patterns and best routes. Sometimes, simple destination-based routing is not sufficient. In these cases, network designers may route packets based on source addresses, protocol types, or application type so that they can optimally shape traffic patterns.

Objectives

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

- List the advantages of PBR
- Describe how PBR is implemented using route maps
- Configure PBR
- Use the **show** and **debug** commands to verify PBR

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Benefits of Policy-Based Routing**
- **Establishing PBR Route Maps**
- **Example of a PBR Configuration**
- **Using PBR show and debug Commands**
- **Summary**
- **Quiz**

Benefits of Policy-Based Routing

This topic defines PBR and discusses several of the key benefits that it provides.

Policy-Based Routing

Cisco.com

- **PBR allows you to implement policies that selectively cause packets to take different paths.**
 - IP routing is typically destination-based.
 - PBR allows for source-based routing.
- **You can also mark traffic with different type of service (ToS) configurations.**
- **PBR requires a route map to implement policy.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-4

PBR offers significant benefits in terms of implementing user-defined policies to control traffic in the internetwork. It provides solutions in cases where legal, contractual, or political constraints dictate that traffic be routed through specific paths.

PBR adds flexibility in a difficult-to-manage environment by providing the network administrator the ability to route traffic based on network needs. For network managers who implement routing policies in their networks, PBR provides an extremely powerful, simple, and flexible tool.

PBR also provides a mechanism to mark packets. As a result, differentiated preferential service can be provided to different types of traffic in combination with queuing techniques available in Cisco IOS software.

Policy-Based Routing Benefits

Cisco.com

PBR has the following benefits:

- **Source-based transit provider selection**
 - Different users go different ways
- **QoS**
 - Sets precedence or ToS; used with queuing
- **Load sharing**
 - Forces load sharing without regard to routing table
- **Cost savings**
 - Distributes traffic economically

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-6

The following benefits are achieved by implementing PBR in a network:

- **Source-based transit provider selection:** Internet service providers (ISPs) and other organizations use PBR to route traffic originating from different sets of users through different Internet connections across the policy routers.
- **Quality of service (QoS):** Organizations provide QoS to differentiated traffic using the following two methods:
 - Setting the precedence or ToS values in the IP packet headers at the periphery of the network
 - Leveraging queuing mechanisms to prioritize traffic in the core or backbone of the network
- **Cost savings:** Organizations achieve cost savings by distributing interactive and batch traffic among low-bandwidth, low-cost, permanent paths and high-bandwidth, high-cost, switched paths.
- **Load sharing:** In addition to the dynamic load-sharing capabilities that are offered by destination-based routing that is supported by IOS software, network managers can implement policies to distribute traffic among multiple paths based on the traffic characteristics.

Establishing PBR Route Maps

PBR uses route maps to implement routing policy. This topic defines the primary route map commands that are required to configure PBR.

Defining Policies Using a Route Map

Cisco.com

- **Applied to incoming packets**
- **Implemented using route maps as follows:**
 - Matching routes are modified by set commands.
 - If match criteria are met and route map specifies permit, use policy route that is specified by the set commands.
 - If match criteria are met and route map specifies deny, use normal (destination-based) routing.
 - If all sequences in the list have been checked and there are no matches, use normal (destination-based) routing.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-6

PBR is applied to incoming packets. All packets received on an interface that has PBR enabled are considered for PBR. Enabling PBR prompts the router to evaluate incoming packets using a route map configured for that purpose. Based on the criteria that are defined in the route map, packets are forwarded to the appropriate next hop. Therefore, these criteria override the normal routing procedures of the router.

Routers typically forward packets to destination addresses based on the information in their routing tables. Instead of routing according to the destination address, PBR allows network administrators to determine and implement routing policies based on the following criteria:

- Identity of a particular end system
- Application being run
- Protocol in use
- Size of packets

The route map statements that are used for PBR are marked as “permit” or “deny,” and are implemented as follows:

- If the statement is marked as “deny,” a packet that meets the match criteria is processed through the normal forwarding channels (destination-based routing is performed).
- If the statement is marked as “permit” and the packet meets the match criteria, then the **set** commands are applied. If no match is found in the route map, the packet is not dropped; it is forwarded through the normal forwarding channel, which means that destination-based routing is performed.
- If the router is required to drop packets that do not match the criteria (instead of being able to forward them normally), then a set statement to route those packets to the null0 interface should be specified as the last entry in the route map.

Policy Routing match Commands

Cisco.com

```
Router(config-route-map)#  
match ip address {access-list-number | name}  
[...access-list-number | name]
```

- Matches IP addresses for policy routing

```
Router(config-route-map)#  
match length min max
```

- Matches Layer 3 length of packet for policy routing

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-7

IP standard or extended access lists are used to establish PBR match criteria using the **match ip address** command. A standard IP access list is used to specify match criteria for the source address of a packet. Extended access lists are used to specify match criteria based on source and destination addresses, application, protocol type, ToS, and precedence.

Table 1: The match ip address Command Parameters

Parameters	Description
<i>access-list-number name</i>	The number or name of a standard or extended access list that is used to test incoming packets. If multiple access lists are specified, matching any one will result in a match.

The **match length** command is used to establish criteria based on the packet length between specified minimum and maximum values. For example, a network administrator uses the match length as the criterion that distinguishes between interactive and file transfer (bulk) traffic because file transfer traffic typically has larger packet sizes.

Table 2: The match length Command Parameters

Parameter	Description
<i>max</i>	Maximum Layer 3 length of the packet, inclusive, that is allowed for a match.
<i>min</i>	Minimum Layer 3 length of the packet, inclusive, that is allowed for a match.

Policy Routing set Commands

Cisco.com

```
Router(config-route-map)#
  set ip next-hop ip-address [...ip-address]
```

- Defines next hop to output packets

```
Router(config-route-map)#
  set interface type number [...type number]
```

- Defines interface to output packets that have an explicit route to the destination

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-8

If the match statements are satisfied, one or more of the following set statements are used to specify the criteria for forwarding packets through. The router evaluates the four **set** commands for PBR that are shown in this figure and the following figure, in the order listed.

Once a destination address or interface is chosen, other **set** commands for changing the destination address or interface are ignored. However, some of these commands affect only packets for which there is an explicit route in the routing table, and others affect only packets for which there is *no* explicit route in the routing table.

A packet that is not affected by any of the **set** commands in a route map statement is not policy-routed, and it is forwarded normally. In other words, destination-based routing is performed. The router uses the four **set** commands for PBR in the following order:

1. The **set ip next-hop** command configures a list of IP addresses. The list specifies the adjacent next-hop router in the path toward the destination to which the packets are forwarded. If more than one IP address is specified, then the first IP address that is associated with a currently active interface is used to route the packets.

Note With the **set ip next-hop** command, the routing table is checked only to determine if the next hop is reachable, but it is not checked to determine if there is an explicit route for the destination address of the packet.

This **set** command affects all packet types and is always used if it is configured.

Table 3: The set ip next-hop Command Parameters

Parameter	Description
<i>ip-address</i>	The IP address of the next hop to which packets are output. It must be the address of an adjacent router.

2. The **set interface** command configures a list of interfaces through which the packets are routed. If more than one interface is specified, then the first active interface in the list is used for forwarding the packets.

Note If there is no explicit route in the routing table for the destination network address of the packet (for example, if the packet is a broadcast packet or is destined to an unknown address), the **set interface** command has no effect and is ignored.

A default route in the routing table will not be considered an explicit route for an unknown destination address.

Table 4: The set interface Command Parameters

Parameter	Description
<i>type number</i>	The interface type and number to which packets are output.

Policy Routing set Commands (Cont.)

Cisco.com

```
Router(config-route-map)#
  set ip default next-hop ip-address [...ip-address]
```

- Defines next hop to output packets that have no explicit route to the destination

```
Router(config-route-map)#
  set default interface type number [...type number]
```

- Defines interface to output packets that have no explicit route to the destination
- Recommended only for point-to-point links

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-9

3. The **set ip default next-hop** command configures a list of default next-hop IP addresses if there is no explicit route available to the destination address of the packet being considered for PBR. If more than one IP address is specified, then the first next hop specified that appears to be adjacent to the router is used. The optional specified IP addresses are tried in turn.

Note A packet is routed to the next hop specified by the **set ip default next-hop** command if there is no explicit route for the destination address of the packet in the routing table.

A default route in the routing table will not be considered an explicit route for an unknown destination address.

Table 5: The set ip default next-hop Command Parameters

Parameter	Description
<i>ip-address</i>	The IP address of the next hop to which packets are output. It must be the address of an adjacent router.

4. The **set default interface** command configures a list of default interfaces. If there is no explicit route available to the destination address of the packet that is being considered for PBR, then it is routed to the first active interface in the list of specified default interfaces.

Note	A packet is routed out of the interface that is specified by the set default interface command only if there is no explicit route for the destination address of the packet in the routing table.
	A default route in the routing table will not be considered an explicit route for an unknown destination address.

Table 6: The set default interface Command Parameters

Parameter	Description
type number	The interface type and number to which packets are output.

PBR also provides a mechanism to mark packets using the **set ip tos** and **set ip precedence** commands:

- The **set ip tos** command is used to set the IP ToS value in the IP packets.
- The **set ip precedence** command is used to set the IP precedence in the IP packets. You must specify either the precedence number or name.

Note	The set commands can be used in conjunction with each other.
-------------	---

Configuring Policy-Based Routing

Cisco.com

```
Router(config-if)#  
ip policy route-map map-tag
```

- Specifies a route map to use for policy routing on an incoming interface that is receiving the packets that need to be policy-routed

```
Router(config-if)#  
ip route-cache policy
```

- Enables fast-switched policy routing

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-10

To identify a route map to use for PBR on an interface, use the **ip policy route-map** interface configuration command.

Table 7: The ip policy route-map Command Parameters

Parameter	Description
<i>map-tag</i>	The name of the route map to use for PBR. It matches a route map name specified by a route-map command.

Note PBR is specified on the incoming interface that receives the packets that need to be policy-routed, not on the interface from which the packets are sent.

Since Cisco IOS Release 12.0, IP PBR can now be fast-switched. Prior to this feature, PBR was process-switched, which meant that on most platforms, the switching rate was approximately 1000 to 10,000 packets per second (pps). This rate was not fast enough for many applications.

Users who require PBR to occur at faster speeds can now implement it without slowing down the router.

PBR must be configured before PBR fast switching can be enabled. Fast switching of PBR is disabled by default. To configure fast-switched PBR, use the **ip route-cache policy** command in interface configuration mode.

Fast-switched PBR supports all of the **match** commands and most of the **set** commands, except for the following restrictions:

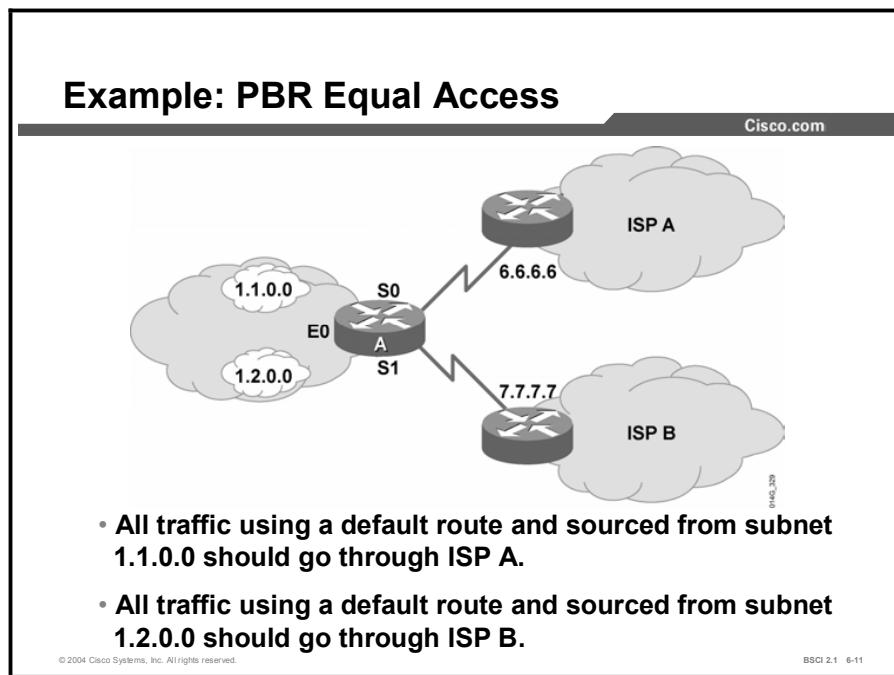
- The **set ip default next-hop** command is not supported.

- The **set interface** command is supported over point-to-point links, unless a route cache entry exists that uses the same interface that is specified in the **set interface** command in the route map. Also, at the process level, usually the routing table is checked to determine if the interface is on an appropriate path to the destination.

During fast switching, the software does not make this check. Instead, if the packet matches, the software automatically forwards the packet to the specified interface.

Example of a PBR Configuration

This topic describes one example of how to use PBR. This example describes a common scenario where a private company that is attached to more than one ISP must build a traffic policy.



In this figure, router A provides Internet access for a private enterprise. Router A is connected to two different ISPs. This router is advertising a 0.0.0.0 default route into the enterprise network to avoid a large Internet routing table.

The problem is that when traffic from the enterprise networks 1.1.0.0 and 1.2.0.0 reaches router A, the traffic can go to ISP A or ISP B. The company prefers to have ISP A and ISP B receive approximately equal amounts of traffic. PBR is used to shape or load-balance traffic from router A to each of the ISPs.

PBR is implemented at router A. All traffic sourced from the 1.1.0.0 subnet is forwarded to ISP A if there is no specific route to the destination in the routing table (the default route is not used). All traffic sourced from the 1.2.0.0 subnet is forwarded to ISP B if there is no specific route to the destination in the routing table.

Note	Remember, this policy provides for an outbound traffic policy from the enterprise to its ISPs only. It does not determine the inbound traffic policy for router A. It is possible that traffic from 1.1.0.0 going out to ISP A will receive responses from ISP B.
-------------	---

Example: PBR Equal Access (Cont.)

Cisco.com

```
RouterA(config)# access-list 1 permit ip 1.1.0.0 0.0.255.255
RouterA(config)# access-list 2 permit ip 1.2.0.0 0.0.255.255

RouterA(config)# route-map equal-access permit 10
RouterA(config-route-map)# match ip address 1
RouterA(config-route-map)# set ip default next-hop 6.6.6.6
RouterA(config-route-map)# route-map equal-access permit 20
RouterA(config-route-map)# match ip address 2
RouterA(config-route-map)# set ip default next-hop 7.7.7.7
RouterA(config-route-map)# route-map equal-access permit 30
RouterA(config-route-map)# set default interface null0

RouterA(config)# interface ethernet 0
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
RouterA(config-if)# ip policy route-map equal-access

RouterA(config)# interface serial 0
RouterA(config-if)# ip address 6.6.6.5 255.255.255.0

RouterA(config)# interface serial 1
RouterA(config-if)# ip address 7.7.7.6 255.255.255.0
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-12

The configuration that is shown in the figure has been set in router A. The name of the route map is “equal-access.”

The **ip policy route-map equal-access** command has been applied to the Ethernet 0 interface, which is the incoming interface receiving the packets to be policy-routed.

Sequence number 10 in the route map equal-access is used to match all packets that are sourced from any host in subnet 1.1.0.0. If there is a match, and if the router has no explicit route for the destination of the packet, it is sent to next-hop address 6.6.6.6 (ISP A router).

Sequence number 20 in the route map equal-access is used to match all packets that are sourced from any host in subnet 1.2.0.0. If there is a match, and if the router has no explicit route for the destination of the packet, it is sent to next-hop address 7.7.7.7 (ISP B router).

Sequence number 30 in the route map equal-access is used to drop all traffic that is not sourced from subnet 1.1.0.0 or 1.2.0.0. The null0 interface is a route to nowhere (thus, being dropped).

Using PBR show and debug Commands

This topic describes the **show** and **debug** commands that are used to verify that a configured policy is working correctly.

Verifying Policy-Based Routing

Cisco.com

Router#
show ip policy

- Displays route maps that are configured on interfaces

Router#
show route-map [map-name]

- Displays a route map

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 6-13

To display the route maps used for PBR on the interfaces of the router, use the **show ip policy** EXEC command.

To display configured route maps, use the **show route-map** EXEC command.

Table 8: The show route-map Command Parameters

Parameter	Description
<i>map-name</i>	(Optional) Name of a specific route map.

Verifying Policy-Based Routing (Cont.)

Cisco.com

Router#

```
debug ip policy
```

- Enables display of IP policy routing events

Router#

```
traceroute
```

- Extended traceroute allows specification of source address

Router#

```
ping
```

- Extended ping allows specification of source address

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-14

Use the **debug ip policy** EXEC command to display IP PBR packet activity. This command shows in detail the activities that PBR is performing. It also displays information that indicates whether a packet matches the criteria. If the criteria match, the resulting routing information for the packet is displayed as well.

Note

Because the **debug ip policy** command generates a significant amount of output, use it only when traffic on the IP network is low so that other activity on the system is not adversely affected.

To discover the routes that packets follow when traveling to their destination from the router, use the **traceroute** privileged EXEC command. To change the default parameters and invoke an extended traceroute test, enter the command without a destination argument. You will be guided through a dialog to select the required parameters.

To check host reachability and network connectivity, use the **ping** privileged EXEC command. You can use the extended command mode of the **ping** command to specify the supported header options by entering the command without any arguments.

Verifying Policy-Based Routing Examples

Cisco.com

```
RouterA# show ip policy
Interface      Route map
Ethernet0      equal-access

RouterA# show route-map
route-map equal-access, permit, sequence 10
Match clauses:
  ip address (access-lists): 1
  Set clauses:
    ip default next-hop 6.6.6.6
Policy routing matches: 3 packets, 168 bytes
route-map equal-access, permit, sequence 20
Match clauses:
  ip address (access-lists): 2
  Set clauses:
    ip default next-hop 7.7.7.7
route-map equal-access, permit, sequence 30
Set clauses:
  default interface null0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-18

Note The output in the figure is from router A in the last example.

In the figure, the output provides examples of two **show** commands. The **show ip policy** command indicates that the route map called equal-access is used for PBR on the Ethernet0 interface of the router.

The **show route-map** command indicates that three packets have matched sequence 10 of the route map equal-access.

Verifying Policy-Based Routing Examples (Cont.)

Cisco.com

```
RouterA# debug ip policy
Policy routing debugging is on

11:51:25: IP: s=1.1.1.1 (Ethernet0), d=190.168.1.1, len 100,
policy match
11:51:25: IP: route map equal-access, item 10, permit
11:51:25: IP: s=1.1.1.1 (Ethernet0), d=190.168.1.1
(Serial0), len 100, policy routed
11:51:25: IP: Ethernet0 to Serial0 6.6.6.6
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-16

Note The output in the figure is from router A in the last example.

In the figure, the output provides an example of the **debug ip policy** command. The **show logging** command shows the logging buffer, including the output of the **debug** command.

The output indicates that a packet from 1.1.1.1 destined for 190.168.1.1 has been received on interface Ethernet0 and that it is policy-routed on Serial0 to next hop 6.6.6.6. The source address of 1.1.1.1 matches line 10 of the route map equal-access.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **PBR offers significant benefits in terms of implementing user-defined policies to control traffic in the internetwork. The benefits achieved by implementing PBR in a network include source-based transit provider selection, QoS, cost savings, and load sharing.**
- **PBR uses route maps to implement routing policy. PBR match criteria are established using the match ip address and match length commands. Various set commands are used to specify the criteria for forwarding packets through the router.**
- **PBR is sometimes implemented on a router to manage traffic to ISPs. PBR is used to shape or load-balance traffic from routers to a number of ISPs.**
- **PBR show and debug commands are used to verify that a configured policy is working properly.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 6-17

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 6-3: Configuring Policy-Based Routing (Optional)

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 feature is NOT a benefit of PBR?

- A) cost savings
- B) load sharing
- C) source-based routing
- D) destination-based routing
- E) QoS

Q2) Which four matching parameters does PBR use to determine policy for a packet?
(Choose four.)

- A) packet length
- B) packet source address
- C) routing protocol
- D) application type
- E) bandwidth of the link
- F) protocol type (for example, TCP, UDP, ICMP)

Q3) A policy has been defined in a route map called “test.”

Which syntax will implement that policy on interface serial 1?

- A) under interface serial 1, **ip policy route-map test**
- B) under interface serial 1, **ip policy test**
- C) under global configuration, **ip policy test interface serial 1**
- D) under global configuration, **ip policy route-map test interface serial 1**

Q4) Which **show** command is used to determine where PBR has been implemented on the router?

- A) **show ip policy**
- B) **show logging**
- C) **debug ip policy**
- D) **show route map**

Q5) The **debug ip policy** command is used to capture packets as they pass through the policy process within the router.

- A) true
- B) false

Quiz Answer Key

Q1) D

Relates to: Benefits of Policy-Based Routing

Q2) A, B, D, F

Relates to: Establishing PBR Route Maps

Q3) A

Relates to: Establishing PBR Route Maps

Q4) A

Relates to: Using PBR show and debug Commands

Q5) A

Relates to: Using PBR show and debug Commands

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:

- Quiz 6-1: Migration and Route Selection Between Multiple IP Routing Protocols
- Quiz 6-2: Configuring and Verifying Route Redistribution
- Quiz 6-3: Controlling Routing Update Traffic
- Quiz 6-4: Using Route Maps to Control Routing Updates
- Quiz 6-5: Using Administrative Distance to Influence the Route Selection Process
- Quiz 6-6: Policy-Based Routing

Quiz 6-1: Migration and Route Selection Between Multiple IP Routing Protocols

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

Objectives

This quiz tests your knowledge of how to:

- Describe the principles and issues that are involved in migrating from one routing protocol to another
- List planning issues for new IP address allocation
- Describe how to migrate to a scalable IP addressing plan
- Describe how to migrate to a new routing protocol
- Explain why route redistribution is useful
- Compare the seed metrics that are used by different routing protocols
- List the considerations for implementing route redistribution

Quiz

Answer these questions:

- Q1) What is the default seed metric for routes (except BGP routes) that are redistributed into OSPF?
- A) 0
 - B) 10
 - C) 20
 - D) OSPF has no default metric.
- Q2) What is the default seed metric for routes that are redistributed into EIGRP?
- A) 0
 - B) 10
 - C) 20
 - D) EIGRP has no default metric.
- Q3) Which command do you use to configure a secondary IP address on an interface?
- A) router(config)# <ip address> <subnet mask> **secondary**
 - B) router(config-if)# **secondary address**
router(config-if-sec)# <ip address> <subnet mask>
 - C) router(config-if)# <ip address> <subnet mask> **secondary**
 - D) router(config-if)# **no ip address**
router(config-if)# <ip address> <subnet mask> **secondary**
- Q4) Which two problems can incorrect route redistribution cause? (Choose two.)
- A) routing loops
 - B) suboptimal path selection
 - C) router crashes
 - D) broadcast storms

- Q5) Which two methods can you use to protect against the problems that are caused by incorrect redistribution? (Choose two.)
- A) always include RIP as one of the protocols that you are redistributing
 - B) filter the routes that are redistributed
 - C) do two-way redistribution and allow all routers to have knowledge of all routes
 - D) do one-way redistribution at only one router
- Q6) What are three reasons to migrate to a routing protocol that supports VLSM? (Choose three.)
- A) makes the network more scalable
 - B) simplifies configuration by requiring the use of the same subnet mask on all subnets
 - C) conserves IP addresses
 - D) allows for a hierarchical addressing plan
- Q7) When you are transitioning to a new IP addressing plan, what three changes might you need to make to the network? (Choose three.)
- A) update network statements for routing protocols
 - B) configure new address mapping on DNS servers
 - C) temporarily halt the use of DHCP
 - D) change the configurations for devices performing NAT
- Q8) What is the recommended procedure when you are redistributing between two routing protocols?
- A) configure both protocols on all routers
 - B) configure temporary static routes on all routers
 - C) change the protocol timers to allow for a longer convergence time
 - D) choose a router to be the redistribution point and run both protocols on it

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 6-2: Configuring and Verifying Route Redistribution

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

Objectives

This quiz tests your knowledge of how to:

- Describe how to configure route redistribution
- Use the **redistribute** command for RIP
- Use the **redistribute** command for OSPF
- Use the **redistribute** command for EIGRP
- Use the **redistribute** command for IS-IS
- Verify route redistribution operations by inspecting the resulting routing tables

Quiz

Answer these questions:

- Q1) Route redistribution occurs automatically between _____.
A) IGRP and EIGRP with the same AS number on the same router
B) RIPv2 and IPX RIP
C) OSPF and IS-IS, because they are both link-state protocols
D) none of the routing protocols; route redistribution must always be configured—it is never automatic
- Q2) Route redistribution is typically done _____.
A) from the core protocol into the edge protocol
B) from the edge protocol into the core protocol
C) mutually between the edge and core protocols
D) only between two routers running the same routing protocol
- Q3) When you are redistributing routes from OSPF into another protocol, the **match** option allows the narrowing of the redistribution to include which three types of routes?
(Choose three.)
A) routes with a metric matching the specified value
B) internal routes learned natively from OSPF
C) type external-1 routes
D) type external-2 routes
- Q4) In the **metric** option for EIGRP, in what order is the metric given?
A) bandwidth, delay, load, reliability, and MTU
B) load, bandwidth, reliability, MTU, and delay
C) bandwidth, delay, reliability, load, and MTU
D) MTU, reliability, delay, load, and bandwidth

- Q5) What is the default behavior if you do not use the **subnets** option when redistributing routes into OSPF?
- A) redistribute classful routes only
 - B) redistribute routes that are subnets only
 - C) redistribute subnets for natively learned routes, not for external routes
 - D) do not redistribute any routes
- Q6) Which two routing protocols require an AS or process number to be specified when they are being redistributed? (Choose two.)
- A) RIP
 - B) OSPF
 - C) IS-IS
 - D) EIGRP
- Q7) If a metric value is configured as part of the **redistribute** command, and a default metric has also been configured under the routing protocols, what does the router do?
- A) uses the default metric value as the seed metric
 - B) adds the default metric and the metric that is configured under the **redistribution** command to determine the seed metric
 - C) uses the metric that is configured under the **redistribute** command as the seed metric
 - D) does not redistribute the route
- Q8) In Cisco IOS Release 12.1, which two routing protocols require a default metric to be specified for routes to be redistributed from other routing protocols? (Choose two.)
- A) RIPv2
 - B) EIGRP
 - C) OSPF
 - D) IS-IS
- Q9) A router has been configured to redistribute EIGRP routes into OSPF. Which of the following routes are redistributed?
- A) all routes in the EIGRP topology table
 - B) EIGRP routes that are in the routing table and routes for any connected interfaces running EIGRP
 - C) EIGRP routes that are in the routing table
 - D) EIGRP successors and feasible successors
- Q10) Which three options are available when you are redistributing routes into OSPF? (Choose three.)
- A) **metric**
 - B) **metric-type**
 - C) **level**
 - D) **subnets**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 6-3: Controlling Routing Update Traffic

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

Objectives

This quiz tests your knowledge of how to:

- Describe and configure passive interfaces
- Describe and configure route-filtering techniques using distribute lists
- Explain the implementation of the distribute list route-filtering technique

Quiz

Answer these questions:

- Q1) Which command do you use to prevent all routing updates from being advertised out of a specific interface?
- A) **passive-interface** command
 - B) **distribute-list out** command
 - C) **distribute-list in** command
 - D) **redistribute <protocol>** command
- Q2) What is the purpose of the **passive-interface default** command?
- A) When it is given in routing protocol configuration mode, the command causes an interface to default to using that routing protocol if the interface is not listed in the network statement of any other protocols.
 - B) When it is given in interface configuration mode, the command causes the interface to shut down unless the primary route is lost. You can then use the passive interface as a backup route.
 - C) When it is given in interface configuration mode, the command prevents the interface from participating in any routing protocol.
 - D) When it is given in routing protocol configuration mode, the command prevents the router from sending routing updates or hellos out of all interfaces on the router, unless it is modified by the **no passive-interface** command.
- Q3) Which three methods can you use to control or prevent routing updates?
(Choose three.)
- A) static routes
 - B) distribute lists
 - C) default metric
 - D) default routes

- Q4) A router receives a routing update on an interface that is listed in an inbound distribute list. Some of the networks listed in the update are not permitted by the distribute list. What does the router do?
- A) It discards the entire update.
 - B) It allows the permitted networks and discards information about the other networks.
 - C) It allows the entire update as long as it contains information about one permitted network.
 - D) Distribute lists work only for outbound updates, not inbound ones.
- Q5) A router redistributes OSPF routes into EIGRP. What is the correct command to apply a distribute list to these redistributed routes?
- A) Router(config)# **router ospf**
Router(config-router)# **distribute-list 1 out eigrp 100**
 - B) Router(config)# **router eigrp 100**
Router(config-router)# **distribute-list 1 in ospf 100**
 - C) Router(config)# **router eigrp 100**
Router(config-router)# **distribute-list 1 out ospf 100**
 - D) Router(config)# **distribute-list 1 ospf 100 eigrp 100**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 6-4: Using Route Maps to Control Routing Updates

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

Objectives

This quiz tests your knowledge of how to:

- Describe the operation of a route map
- Use route map commands
- Explain how route maps are implemented with route redistribution

Quiz

Answer these questions:

- Q1) When a single **match** command has multiple variables, how does the route map treat each variable?
- A) uses OR logic; at least one variable must match
 - B) uses AND logic; all variables must match
 - C) cannot use multiple variables on a match statement; only a set statement allows this activity
- Q2) When multiple **match** commands exist, how does the route map treat each variable?
- A) uses OR logic; at least one variable must match
 - B) uses AND logic; all variables must match
 - C) cannot use multiple match statements under a route map line; only a set statement allows this activity
- Q3) Using a **match ip address** command requires an access list number as the variable; an individual IP address is not allowed.
- A) true
 - B) false
- Q4) Exhibit A:

R2:

```
router eigrp 7
    network 181.16.2.0
    redistribute rip route-map rip-to-eigrp
    default-metric 1 1 1 1 1
router rip
    version 2
    network 178.1.10.0
    redistribute eigrp 7 route map eigrp-to-rip
    default-metric 2
    route-map rip-to-eigrp deny 10
        match tag 88
    route-map rip-to-eigrp permit 20
        set tag 77
```

```

route-map eigrp-to-rip deny 10
  match tag 77
route-map eigrp-to-rip permit 20
  set tag 88

```

Based on Exhibit A, how will RIP be redistributed into EIGRP?

- A) All routes will be redistributed with a tag of 77.
 - B) All routes will be redistributed with a tag of 88.
 - C) Those routes not tagged with 88 will be redistributed with a tag of 77.
 - D) Those routes not tagged with 77 will be redistributed with a tag of 88.
- Q5) Based on Exhibit A, what is the **route-map eigrp-to-rip** command designed to do?
- A) Before RIP allows any routes to be redistributed in from EIGRP, it checks the route for tag 77. If RIP finds tag 77, then it denies redistribution because it originated from RIP.
 - B) Before EIGRP allows any routes to be redistributed in from RIP, it checks the route for tag 88. If EIGRP finds tag 88, then it denies redistribution because it originated from EIGRP.
 - C) It keeps RIP from redistributing routes into EIGRP if they are marked with tag 77.
 - D) It allows all routes to redistribute into EIGRP if they are not tagged with 88.
- Q6) A route map has been configured for RIP into OSPF redistribution. When a match is found, the **set** command is **set metric 10**. What does **set metric 10** mean?
- A) set a cost of 10 to all routes that are redistributed into OSPF
 - B) set a hop count of 10 to all routes that are redistributed into RIP
 - C) Set a cost of 10 to all routes that are redistributed into RIP.
 - D) Add 10 more to the cost of OSPF routes.
- Q7) When matching on an IP route source, the route map is looking for _____.
- A) the source address of the client sending the data packet
 - B) the source address of the adjacent router sending a data packet
 - C) the source address of the adjacent router sending a routing update packet
 - D) the IP address of the router receiving the routing update packet
- Q8) The following match statements exist in a route map permit line:

match ip address 10 20

match ip next-hop 30

What do these statements mean?

- A) A route must match both access list 10 and 20 or next-hop access list 30.
- B) A route must match either access list 10 or 20 or next-hop access list 30.
- C) A route must match either access list 10 or 20 and next-hop access list 30.
- D) A route must match access list 10 or 20 and a next-hop IP address of 30.

Q9) Which three **set** commands are BGP-specific? (Choose three.)

- A) **local-pref**
- B) **weight**
- C) **ip next-hop**
- D) **ip address**
- E) **origin**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 6-5: Using Administrative Distance to Influence the Route Selection Process

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

Objectives

This quiz tests your knowledge of how to:

- List the benefits of manipulating administrative distance
- Use the **distance** commands to modify the default administrative distance of certain routes to influence the route selection process
- Describe the impact of administrative distance changes on routing tables

Quiz

Answer these questions:

Q1) What method is used for assigning an administrative distance to a route?

- A) It is assigned with the **distance** command.
- B) It is assigned with the **redistribute** command.
- C) It is assigned with the **default-metric** command.
- D) It is associated with the **metric** command.

Q2) Routing table excerpt:

```
172.16.3.0 [100/8539] via 172.16.2.2, 00:00:02, TokenRing0
```

In this routing table excerpt, what is the administrative distance?

- A) 100
- B) 8539
- C) 00:00:02

Q3) Choose the correct ranking of the following route sources for trustworthiness. The number in parentheses is the administrative distance.

- A) OSPF (110), EIGRP (90), IS-IS (115), RIP (120), static route (1)
- B) static route (1), EIGRP (90), OSPF (110), IS-IS (115), RIP (120)
- C) RIP (120), IS-IS (115), OSPF (110), EIGRP (90), static route (1)

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 6-6: Policy-Based Routing

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

Objectives

This quiz tests your knowledge of how to:

- List the advantages of PBR
- Describe how PBR is implemented using route maps
- Configure PBR
- Use the **show** and **debug** commands to verify PBR

Quiz

Answer these questions:

- Q1) Which two of the following statements describe how PBR influences QoS? (Choose two.)
- A) ToS bits are set in the IP packet.
 - B) Bandwidth parameters are set on outbound interfaces.
 - C) Precedence bits are set in the IP packet.
 - D) Priority queuing bits are set in the IP packet.
- Q2) PBR improves performance in the router because fast switching for PBR is *on* by default.
- A) true
 - B) false
- Q3) Which of the following variables is not used as a set variable in PBR?
- A) next-hop address
 - B) outbound interface
 - C) precedence bits
 - D) packet length
- Q4) Which two of the following statements describe the differences between **set interface** and **set default interface** in a route map? (Choose two.)
- A) **Set interface** is used when the packet finds a default route in the routing table.
 - B) **Set interface** is used when the packet finds a match in the routing table.
 - C) **Set default interface** is used when the packet does not find a match in the routing table.
 - D) **Set interface** routes packets to a specific interface, and **set default interface** routes packets to a general interface.
- Q5) What is set when you are configuring match length criteria?
- A) minimum packet size only
 - B) maximum packet size only
 - C) minimum and maximum packet size
 - D) average packet size

- Q6) What does the **show ip policy** command do?
- A) displays route maps per interface
 - B) displays the route map
 - C) displays PBR packet activity
 - D) displays PBR console messages

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 6-1: Migration and Route Selection Between Multiple IP Routing Protocols

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

Quiz 6-2: Configuring and Verifying Route Redistribution

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

Quiz 6-3: Controlling Routing Update Traffic

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

Quiz 6-4: Using Route Maps to Control Routing Updates

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

Quiz 6-5: Using Administrative Distance to Influence the Route Selection Process

- Q1) A
- Q2) A
- Q3) B

Quiz 6-6: Policy-Based Routing

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

Module 7

Configuring Basic BGP

Overview

The Internet has become a vital resource in many organizations, resulting in redundant connections to multiple Internet service providers (ISPs). With multiple connections, Border Gateway Protocol (BGP) is an alternative to using default routes to control path selections.

Configuring and troubleshooting BGP can be complex. A BGP administrator must understand the various options involved in properly configuring BGP for scalable internetworking.

Module Objectives

Upon completing this module, you will be able to configure and troubleshoot BGP by applying the various options involved in properly configuring BGP for scalable internetworking.

Module Objectives

Cisco.com

- Define the characteristics of the BGP routing protocol
- Describe BGP concepts and terminology
- Configure BGP operations for scalable internetworks
- Configure route summarization with BGP
- Explain the BGP path selection process
- Set the local preference and multi-exit discriminator BGP attributes using route maps
- Select the best implementation for multihoming autonomous systems

Module Outline

The outline lists the components of this module.

Module Outline

Cisco.com

- **BGP Overview**
- **BGP Concepts and Terminology**
- **Basic BGP Operations**
- **BGP Route Summarization**
- **BGP Path Selection Process**
- **Basic BGP Path Manipulation Using Route Maps**
- **Design Options for Multihoming**
- **Lesson Assessments**

BGP Overview

Overview

This lesson introduces Border Gateway Protocol (BGP) as an exterior gateway protocol and describes how BGP routes between autonomous systems. It defines the term “autonomous system” (AS) as it relates to BGP and internal gateway protocols. This lesson also examines various aspects of BGP, such as how it is a path-vector routing protocol and how that functionality enables policy-based routing (PBR). Other characteristics, such as how BGP uses TCP as its transport function, are defined along with the four message types that BGP uses to communicate with other BGP routers.

Relevance

This lesson introduces the key concepts of BGP and identifies the differences between it and the Interior Gateway Protocols (IGPs), such as Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Intermediate System-to-Intermediate System (IS-IS). If you are familiar with the important characteristics of BGP and know that it does not behave as an IGP, then you can better understand when and when not to use BGP.

Objectives

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

- Define BGP and describe the function of an AS
- Describe PBR using BGP path-vector functionality
- Describe the characteristics of BGP
- List the BGP message types

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

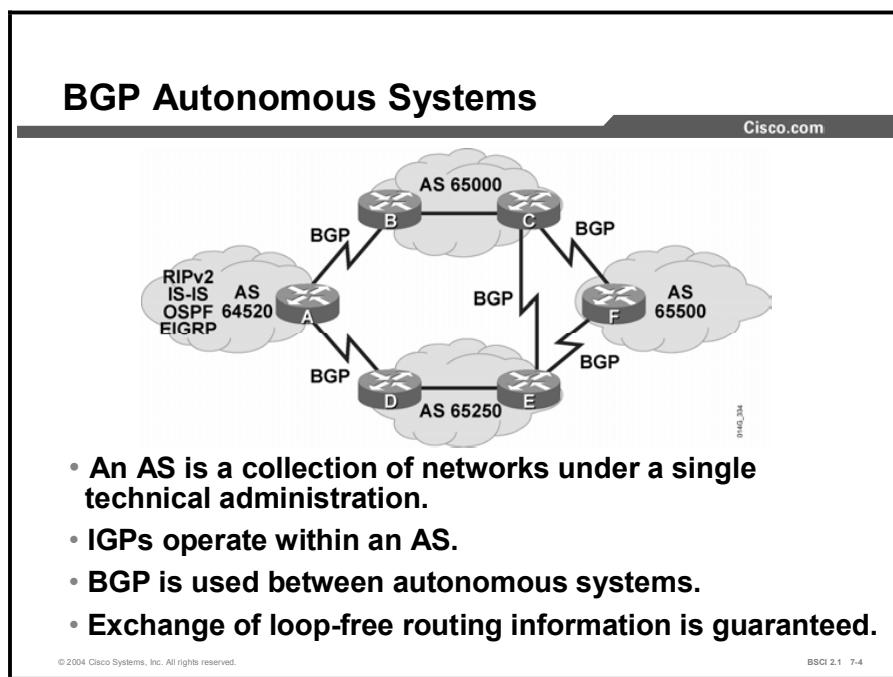
Outline

Cisco.com

- **Overview**
- **Definition of BGP**
- **BGP Path-Vector Routing**
- **BGP Characteristics**
- **BGP Message Types**
- **Summary**
- **Quiz**

Definition of BGP

This topic identifies BGP as an external gateway protocol and defines an Exterior Gateway Protocol (EGP) as compared to an Interior Gateway Protocol (IGP). You need to learn about autonomous systems before you can understand EGPs.



The main goal of BGP is to provide an interdomain routing system that guarantees loop-free exchange of routing information between autonomous systems. Routers exchange information about paths to destination networks.

BGP is a successor of EGP. EGP was developed to isolate networks from each other as the Internet grew.

There are many RFCs relating to BGP version 4 (BGP4), the current version of BGP, including 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, and 2439.

BGP4 has many enhancements over earlier protocols. The Internet uses BGP4 extensively to connect ISPs and to connect enterprises to ISPs.

BGP4 and its extensions are the only acceptable version of BGP available for use on the public-based Internet. BGP4 carries a network mask for each advertised network and supports both variable-length subnet masking (VLSM) and classless interdomain routing (CIDR). BGP4 predecessors did not support these capabilities, which are currently mandatory on the Internet.

When using CIDR on a core router for a major ISP, the IP routing table, which is composed mostly of BGP routes, has more than 120,000 CIDR blocks. Not using CIDR at the Internet level causes the IP routing table to have more than 2,000,000 entries.

Using BGP4, and therefore CIDR, prevents the Internet routing table from becoming too large for interconnecting millions of users.

Routing protocols are categorized as either interior or exterior as follows:

- **IGP:** A routing protocol that exchanges routing information within an AS. Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Enhanced Interior Gateway Routing Protocol (EIGRP) are examples of IGPs.
- **EGP:** A routing protocol that connects different autonomous systems. BGP is an example of an EGP.

BGP is an Interdomain Routing Protocol (IDRP), also known as an external gateway protocol. All of the routing protocols that have been discussed thus far in this course are Interior Gateway Protocols, or IGPs.

BGP4 is the latest version of BGP. As noted in RFC 1771, the classic definition of an AS is “a set of routers under a single technical administration, using an IGP and common metrics to route packets within the autonomous system, and using an EGP to route packets to other autonomous systems.”

Autonomous systems can use more than one IGP, potentially with several sets of metrics. From the BGP point of view, the most important characteristics of an AS are that it appears to other autonomous systems to have a single coherent interior routing plan and presents a consistent picture of reachable destinations. All parts of an AS must connect to each other.

The Internet Assigned Numbers Authority (IANA) is the organization responsible for allocating AS numbers. Specifically, the American Registry for Internet Numbers (ARIN) has the jurisdiction to assign numbers for the Americas, the Caribbean, and Africa. Réseaux IP Européennes Network Information Center (RIPENIC) administers AS numbers for Europe, and the Asia Pacific Network Information Center (APNIC) administers the numbers for the Asia-Pacific region.

AS numbers are 16-bit numbers ranging from 1 to 65535; RFC 1930 provides guidelines for the use of AS numbers. A range of AS numbers, 64512 through 65535, is reserved for private use, much like private IP addresses.

Note	Using an IANA-assigned AS number rather than a private AS number is necessary only if your organization plans to use an external gateway protocol such as BGP, and connect to a public network, such as the Internet.
-------------	---

An internal routing protocol looks for the quickest path from one point in a corporate network to another, based upon certain metrics. RIP uses hop counts that look to cross the least number of Layer 3 devices to reach the destination network. OSPF and EIGRP look for the best speed according to the bandwidth statement of the interface. All internal routing protocols look at outbound cost to get somewhere.

BGP, an external routing protocol, does not look at speed for the best path. BGP is a policy-based routing (PBR) protocol that allows an AS to control traffic flow across its wires using multiple BGP path attributes. It allows a provider to fully use all its bandwidth by path manipulation.

BGP Path-Vector Routing

This topic explains the concept of a path-vector routing protocol as opposed to a distance vector or link-state routing protocol.

BGP Path-Vector Routing

Cisco.com

Path Advertised:
64200 64600 64700
Networks in 64700:
192.168.24.0
192.168.25.0
172.20.0.0

- **IGPs announce networks and describe the cost to reach those networks.**
- **BGP announces pathways and the networks that are reachable at the end of the pathway. BGP describes the pathway by using attributes, which are similar to metrics.**
- **BGP allows administrators to define policies or rules for how data will flow through the autonomous systems.**

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 7-5

BGP routers exchange network reachability information, called path vectors, made up of path attributes. The path-vector information includes a list of the full path of BGP AS numbers necessary to reach a destination network.

This AS path information is useful to construct a graph of loop-free autonomous systems and is used to identify routing policies so that restrictions on routing behavior can be enforced based on the AS path.

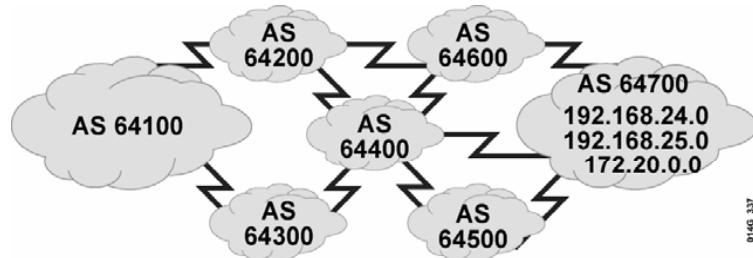
Internal routing protocols announce a list of networks and the metrics to get to each network. BGP announces the AS (hop-by-hop) pathway to a destination AS. BGP describes this pathway using attributes, such as the IP address, to get to the next AS (next-hop attribute) and to indicate how the networks at the end of the pathway were introduced into BGP (origin code attribute).

Many other BGP attributes, besides next hop and origin code, are also used to describe the pathway and the networks at the end of the pathway.

The AS path is always loop-free because a router running BGP does not accept a routing update that already includes its AS number in the path list. The router does not accept the routing update because the update has already passed through its AS, and accepting it again would result in a routing loop.

BGP Policy-Based Routing

Cisco.com



- **BGP can support any policy conforming to the hop-by-hop (AS-by-AS) routing paradigm.**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

BGP allows routing-policy decisions at the AS level to be enforced. These policies can be implemented for all networks owned by an AS, for a certain CIDR block of network numbers (prefixes), or for individual networks or subnetworks.

BGP specifies that a BGP router can advertise to neighboring autonomous systems only those routes that it uses itself. This rule reflects the hop-by-hop routing paradigm that the Internet generally uses.

The hop-by-hop routing paradigm does not support all possible policies. For example, BGP does not enable one AS to send traffic to a neighboring AS, intending that the traffic take a different route from that taken by traffic that originates in the neighboring AS.

In other words, you cannot influence how a neighboring AS routes traffic, but you can influence how your traffic gets to a neighboring AS. BGP supports any policy that conforms to the hop-by-hop routing paradigm.

Because the Internet currently uses the hop-by-hop routing paradigm only, and because BGP can support any policy that conforms to that paradigm, BGP is highly applicable as an inter-AS routing protocol.

Example

For example, the following pathways are possible for AS 64100 to reach networks in AS 64700 through AS 64200:

- 64200 64600 64700
- 64200 64600 64400 64500 64700
- 64200 64600 64400 64300 64500 64700
- 64200 64400 64600 64700
- 64200 64400 64500 64700
- 64200 64400 64300 64500 64700

AS 64100 does not see all these possibilities.

AS 64200 advertises to AS 64100 only its best pathway of 64200 64600 64700, the same way that IGP announce only their best least-cost routes. This pathway is the only pathway through AS 64200 that AS 64100 sees. All packets that are destined for 64700 through 64200 will take this pathway.

Even though other pathways exist, AS 64100 can only use what AS 64200 advertises for the networks in AS 64700. The AS path that is advertised, 64200 64600 64700, is the AS-by-AS (hop-by-hop) pathway that AS 64200 will use to reach the networks in AS 64700.

To reach the networks in AS 64700, AS 64100 can choose to use AS 64200 or it can choose to go through the pathway that AS 64300 is advertising.

AS 64200 will not announce the other pathway, such as 64200 64400 64600 64700, because it did not choose that as the best pathway based on the BGP routing policy that AS 64200 set up.

AS 64100 will not learn of the second-best pathway, or any other pathways, unless the best pathway of AS 64200 becomes unavailable.

Even if AS 64100 were aware of the other pathway through AS 64200 and wanted to use it, AS 64200 would not route packets along the 64200 64400 64600 64700 pathway because AS 64200 selected 64200 64600 64700 as its best pathway and all AS 64200 routers will use that pathway as a matter of BGP policy.

BGP does not enable one AS to send traffic to a neighboring AS, intending that the traffic take a different route from that taken by traffic originating in the neighboring AS.

BGP Characteristics

This topic describes the characteristics of BGP and when to use, and not to use, BGP.

BGP Characteristics

Cisco.com

- **BGP is most appropriate when at least one of the following conditions exists:**
 - An AS allows packets to transit through it to reach other autonomous systems (e.g., a service provider).
 - An AS has multiple connections to other autonomous systems.
 - Routing policy and route selection for traffic entering and leaving your AS must be manipulated.
- **BGP is not always appropriate. Do not use BGP if you have one of the following conditions:**
 - Single connection to the Internet or other AS
 - Lack of memory or processor power to handle constant updates on BGP routers
 - Limited understanding of route filtering and BGP path selection process
 - Low bandwidth between autonomous systems

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-7

BGP allows ISPs to communicate and exchange packets. These ISPs have multiple connections to each other and agreements to exchange updates. BGP is used to implement the agreements between two or more autonomous systems.

Improper controlling and filtering of BGP updates can potentially allow an outside AS to affect the traffic flow to your AS. It is important to know how BGP operates and how to configure it properly to prevent this situation.

For example, if you are a customer connected to ISP-A and ISP-B (for redundancy), you want to implement a routing policy to ensure that ISP-A does not send traffic to ISP-B via your AS. You do not want to waste valuable resources and bandwidth within your AS to route traffic for your ISPs. You want to be able to receive traffic destined to your AS through each ISP.

BGP is not always an appropriate solution to interconnect autonomous systems. For example, if only one exit path from the AS exists, a default route is the most appropriate solution. In this case, BGP would unnecessarily use router CPU resources and memory.

If the routing policy that you implement in an AS is consistent with the policy in the ISP AS, it is not necessary or desirable to configure BGP in that AS.

BGP Characteristics (Cont.)

Cisco.com

- **BGP is a distance-vector protocol with the following enhancements:**
 - Reliable updates: BGP runs on top of TCP (port 179)
 - Incremental, triggered updates only
 - Periodic keepalive messages to verify TCP connectivity
 - Rich metrics (called path vectors or attributes)
 - Designed to scale to huge internetworks (e.g., the Internet)

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 7-8

BGP is categorized as an advanced distance vector protocol, but it is actually a path-vector protocol. BGP is very different from standard distance vector protocols like RIP.

BGP uses TCP as its transport protocol, which provides connection-oriented reliable delivery. BGP assumes that its communication is reliable; therefore, it does not have to implement retransmission or error recovery mechanisms. BGP uses TCP port 179. Two routers using BGP form a TCP connection with one another and exchange messages to open and confirm the connection parameters. These two BGP routers are called peer routers, or neighbors.

BGP peers exchange full routing tables after a connection is made. However, because the connection is reliable, BGP peers send only changes (incremental, or triggered, updates) after they make the connection and exchange the full routing table one time. Reliable links do not require periodic routing updates; therefore, routers use triggered updates instead. BGP sends keepalive messages, similar to the hello messages sent by OSPF, IS-IS, and EIGRP.

BGP is the only IP routing protocol to use TCP as its transport layer. OSPF, IGRP, and EIGRP reside directly above the IP layer, and RIP v1 and RIPv2 use User Datagram Protocol (UDP) for their transport layer.

OSPF and EIGRP have their own internal function to ensure that update packets are explicitly acknowledged. These protocols use a one-for-one window so that if either OSPF or EIGRP has multiple packets to send, the next packet cannot be sent until they receive an acknowledgment from the first update packet.

This process can be very inefficient and cause latency issues if thousands of update packets must be exchanged over relatively slow serial links. OSPF and EIGRP rarely have thousands of update packets to send.

EIGRP can hold more than 100 networks in one EIGRP update packet. One hundred EIGRP update packets can hold up to 10,000 networks, and most organizations do not have 10,000

subnets in their corporations. BGP, on the other hand, has more than 120,000 networks to advertise.

TCP handles the acknowledgment function for BGP. TCP uses a dynamic window, which allows for 65,576 bytes to be outstanding before it stops and waits for an acknowledgment.

Thus if BGP sends 1000-byte packets, it does not have to wait for the first packet to be acknowledged before it sends the second packet. With 1000-byte packets and a 65,000-byte window, there would need to be 65 packets that have not been acknowledged for BGP to have to stop and wait for an acknowledgment.

TCP is designed to use a sliding window, where the receiver will acknowledge at the halfway point of the sending window. This method allows any TCP application to continue to stream packets without having to stop and wait like OSPF or EIGRP would require.

BGP Databases

Cisco.com

- **Neighbor table**
 - List of BGP neighbors
- **BGP forwarding table/database**
 - List of all networks learned from each neighbor
 - Can contain multiple pathways to destination networks
 - Database contains BGP attributes for each pathway
- **IP routing table**
 - List of best paths to destination networks

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-9

BGP keeps its own tables to store BGP information that it receives and sends to other routers.

For BGP to establish an adjacency, you must configure it explicitly for each neighbor. BGP forms a TCP relationship with each of the configured neighbors and keeps track of the state of these relationships by periodically sending a BGP/TCP keepalive message.

Note The BGP sends BGP/TCP keepalives, by default, every 60 sec.

After establishing an adjacency, the neighbors exchange the BGP routes in their IP routing table. These routes are collected from each neighbor, who successfully establishes an adjacency, and are then placed in the BGP topology database, or BGP forwarding database.

All routes that have been learned from each neighbor are placed into the BGP topology database. The best routes for each network are selected from the BGP topology database using the BGP route selection process, and then submitted to the IP routing table.

The IP routing table compares the submitted BGP routes to other possible paths to those networks, if any exist, and the best route, based on administrative distance, is installed in the IP routing table.

External BGP routes (BGP routes learned from an external AS) have an administrative distance of 20. Internal BGP routes (BGP routes learned from within the AS) have an administrative distance of 200.

BGP Message Types

This topic describes the BGP packet or message types and their functions.

BGP Message Types

Cisco.com

BGP defines the following message types:

- **Open**
 - Includes holdtime and BGP router ID
- **Keepalive**
- **Update**
 - Information for one path only (could be to multiple networks)
 - Includes path attributes and networks
- **Notification**
 - When error is detected
 - BGP connection is closed after being sent

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-10

BGP peers initially exchange their full BGP routing tables. Afterwards, incremental updates are sent only after topology changes in the network. BGP peers send keepalive messages to ensure that the connection between the BGP peers still exists; they send notification packets in response to errors or special conditions.

After you establish a TCP connection, the first message sent by each side is an open message. If the open message is acceptable, the side that receives the message sends a keepalive message confirming the open message. After the receiving side confirms the open message and establishes the BGP connection, the BGP peers can exchange any update, keepalive, and notification messages. Here are more details about the different types of BGP messages:

- **Open message:** An open message includes the following information:
 - **Version number:** The suggested version number. The highest common version that both routers support is used. Most BGP implementations today use BGP4.
 - **AS number:** The AS number of the local router. The peer router verifies this information. If it is not the AS number that is expected, the BGP session is torn down.
 - **Holdtime:** Maximum number of seconds that can elapse between the successive keepalive and update messages from the sender. Upon receipt of an open message, the router calculates the value of the hold timer by using whichever is smaller: its configured holdtime or the holdtime that was received in the open message.
 - **BGP router identifier (router ID):** This 32-bit field indicates the BGP identifier of the sender. The BGP identifier is an IP address that is assigned to that router, and it is determined at startup. The BGP router ID is chosen in the same way that the OSPF router ID is chosen: it is the highest active IP address on the router, unless a

loopback interface with an IP address exists. In this case, the router is the highest loopback IP address. The router ID can also be statically configured.

- **Optional parameters:** These parameters are Type, Length, Value (TLV)-encoded. An example of optional parameters is session authentication.
- **Keepalive message:** BGP keepalive messages are exchanged between BGP peers often enough to keep the hold timer from expiring. If the negotiated holdtime interval is 0, then periodic keepalive messages are not sent. A keepalive message consists of only a message header.
- **Update message:** A BGP update message has information on one path only; multiple paths require multiple update messages. All the attributes in the update message refer to that path, and the networks are those that can be reached through it. An update message can include the following fields:
 - **Withdrawn routes:** This list displays IP address prefixes for routes that are withdrawn from service, if any.
 - **Path attributes:** These attributes include the AS path, origin, local preference, and so on. Each path attribute includes the attribute type, attribute length, and attribute value. The attribute type consists of the attribute flags, followed by the attribute type code.
 - **Network-layer reachability information:** This field contains a list of IP address prefixes that are reachable by this path.
- **Notification message:** A BGP notification message is sent when an error condition is detected, and the BGP connection is closed immediately. Notification messages include an error code, an error subcode, and data that is related to the error.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **BGP supports any policy that conforms to the hop-by-hop routing paradigm, which makes it highly applicable as an inter-AS routing paradigm.**
- **BGP is categorized as an advanced distance vector protocol, but is actually a path-vector protocol that performs differently than other standard distance vector protocols.**
- **After BGP peers initially exchange their full BGP routing tables, incremental updates are sent only if the network topology changes.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-11

References

For additional information, refer to these resources:

- RFCs 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, and 2439

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) Upon which component does BGP base selection of the best pathway?
- A) speed
 - B) AS routing policy
 - C) number of routers to reach a destination network
 - D) bandwidth plus delay
- Q2) Which routing method best describes BGP?
- A) distance vector
 - B) link-state
 - C) path-vector
 - D) hybrid of link-state and distance vector
- Q3) Which two conditions are valid reasons to run BGP in an autonomous system? (Choose two.)
- A) The AS is an ISP.
 - B) The AS has only a single connection to another AS.
 - C) Path and packet flow manipulation is required in this AS.
 - D) You have a limited understanding of BGP routing and route filtering.
- Q4) Which BGP message establishes a BGP session and carries the holdtime and the BGP router ID?
- A) BGP update message
 - B) BGP keepalive message
 - C) BGP open message
 - D) BGP notification message

Quiz Answer Key

Q1) B

Relates to: Definition of BGP

Q2) C

Relates to: BGP Path-Vector Routing

Q3) A, C

Relates to: BGP Characteristics

Q4) C

Relates to: BGP Message Types

BGP Concepts and Terminology

Overview

This lesson discusses important terminology that is used in establishing Border Gateway Protocol (BGP) peering relationships. The following terms are explained: BGP speaker, BGP router, BGP neighbor, and BGP peer. This lesson defines external and internal BGP neighbors and the requirements for establishing these relationships. In addition, this lesson examines the difference between an Interior Gateway Protocol (IGP) and an Internal Border Gateway Protocol (IBGP), and explains the reason for fully meshed IBGP neighbors.

Relevance

Understanding the relationship between various types of BGP routers and the common terminology that is used when you are discussing these routers is necessary for troubleshooting connectivity issues between BGP neighbors.

Objectives

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

- Identify the proper terms for describing various BGP routers and their relationships
- Describe the requirements for establishing an external BGP neighbor relationship
- Describe the requirements for establishing an internal BGP neighbor relationship
- State why IBGP route propagation requires fully meshed adjacencies

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Terminology for BGP Neighbor Relationships**
- **External BGP Neighbors**
- **Internal BGP Neighbors**
- **Full Mesh of IBGP Neighbors**
- **Summary**
- **Quiz**

Terminology for BGP Neighbor Relationships

This topic defines key terms that describe the relationships between routers that run BGP. These terms include the generic term “BGP speaker” and the more specific term “BGP neighbor,” also known as a “BGP peer.” Finally, this topic discusses the two different types of BGP neighbors.

Peers = Neighbors

Cisco.com

- A “BGP peer,” also known as a “BGP neighbor,” is a specific term that is used for BGP speakers that have established a neighbor relationship.
- Any two routers that have formed a TCP connection to exchange BGP routing information are called peers, or neighbors.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-4

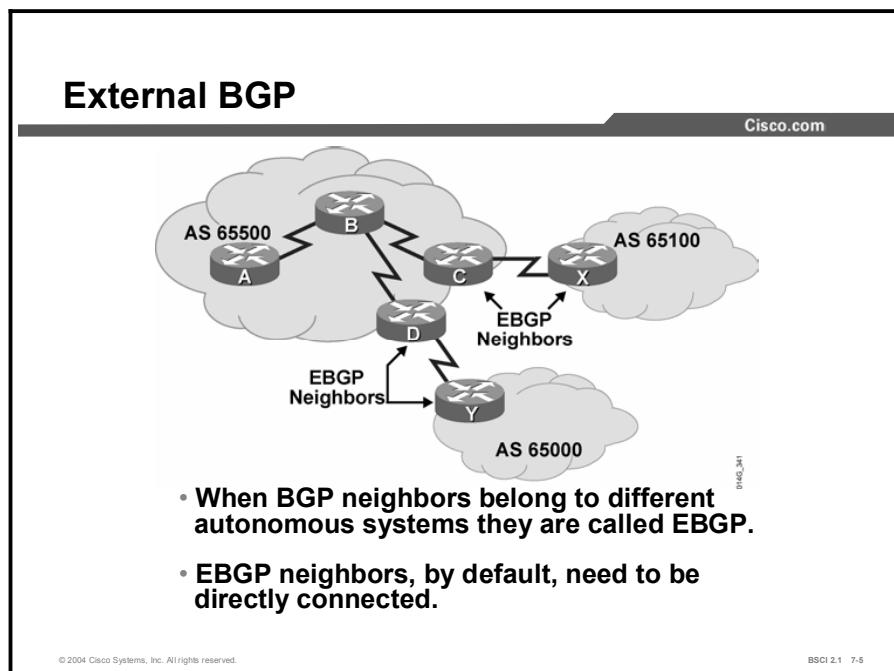
No one router can handle communications with all the routers that run BGP. There are more than 20,000 routers that run BGP and are connected to the Internet, representing more than 10,000 autonomous systems. A BGP router forms a direct neighbor relationship with a limited number of other BGP routers. Through these BGP neighbors, a BGP router learns of the pathways through the Internet to reach any advertised network. Any router that runs BGP is known as a BGP speaker.

The term “BGP peer” has a specific meaning: a BGP speaker that is configured to form a neighbor relationship with another BGP speaker for the purpose of directly exchanging BGP routing information with each other. A BGP speaker has a limited number of BGP neighbors with which it peers and forms a TCP-based relationship.

A BGP peer must be configured with a **bgp neighbor** command. The administrator instructs the BGP speaker to establish a relationship with the address listed in the neighbor statement and to exchange the BGP routing updates with that neighbor. BGP peers are also known as neighbors and can be either internal or external to the AS.

External BGP Neighbors

This topic defines a specific type of BGP peer known as an External BGP (EBGP) neighbor and describes the requirements for establishing an EBGP session.



BGP that runs between routers in different Autonomous Systems is called External BGP (EBGP). By default, routers running EBGP are directly connected to each other.

An internal routing protocol is not run between the EBGP neighbors. When using the BGP neighbor statement, the address that the router points to for establishing the EBGP neighbor relationship must be reachable without using a routing protocol. This address manipulation can be accomplished by pointing at an address that is reachable through a directly connected network or by using static routes to that IP address. Generally, the neighbor address that is used is a directly connected address of the other router.

BGP uses TCP port 179. For two routers to exchange BGP routing updates, the TCP-reliable transport layer on each side must successfully pass the TCP three-way handshake before the BGP session can be established.

Under the router BGP process, you identify which routers to exchange BGP updates with by configuring the neighbor statement with the IP address of the appropriate neighbor. Because the TCP handshaking must take place before a BGP update can be exchanged between two neighbors, the IP address that is used in the neighbor statement must be reachable without using an IGP. An external BGP neighbor is a router outside this AS, such as an ISP, and an internal routing protocol will not be used between the autonomous systems. Thus, BGP cannot be used to pass routing information between the autonomous systems. In this case, the IP address in the neighbor statement must already be reachable before BGP sets up a session with that neighbor or the routers cannot exchange TCP handshaking to establish the BGP session.

Internal BGP Neighbors

This topic defines the second specific BGP peer known as an IBGP neighbor and describes the requirements for establishing an IBGP session.

Internal BGP

- **IGBP refers to the presence of BGP neighbors within the same AS.**
- **The neighbors do not have to be directly connected.**

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 7-6

BGP that runs between routers within the same AS is called IBGP. IBGP runs within an AS to exchange BGP information so that all BGP speakers have the same routing information with regards to outside autonomous systems.

Using the BGP neighbor statement, the address that BGP points to for an IBGP neighbor must be reachable. The IBGP neighbor can be reached by a directly connected network, static routes, or by the internal routing protocol. If the internal routing protocol has installed a route to the IBGP neighbor in the routing table, then TCP can perform its handshaking so BGP can set up its neighbor relationship. Because multiple paths within the AS can usually reach the other IBGP routers in the AS, a loopback address is generally used in the BGP neighbor statement for establishing the IBGP sessions.

Example

When multiple routers in an AS are running BGP, they exchange BGP routing updates with one another. In the figure, routers A, D, and C learn the pathways to the external autonomous systems from their respective EBGP neighbors (Z, Y, and X). If the link between D and Y goes down, D must learn new routes to the external autonomous systems. Other BGP routers within AS 65500 that were using D to get to external networks must also be informed that the pathway through D is not available. Those BGP routers within AS 65500 need to have the alternate pathways through routers A and C in their BGP forwarding database. You must set up IBGP sessions between all routers in AS 65500 so each router within the AS learns about paths to the external networks via IBGP.

Full Mesh of IBGP Neighbors

This topic discusses the need to create fully meshed TCP sessions between all BGP routers within the same AS. This topic compares IBGP behavior with that of an IGP.

IBGP and Redistribution

The diagram shows three Autonomous Systems (ASes) connected by EBGP sessions: AS 65101 (routers A and B), AS 65102 (routers B, C, D, E, and F), and AS 65103 (router F). Router B is the border router between AS 65101 and AS 65102. Router C is an interior router in AS 65102. Router D is another border router between AS 65102 and AS 65103. Router E is an interior router in AS 65102. Router F is the border router between AS 65102 and AS 65103. Router B runs both BGP and OSPF. Router D runs BGP and OSPF. Router E runs BGP and OSPF. Router F runs BGP and OSPF. Router A runs OSPF. Router C runs OSPF. Router D runs BGP and OSPF. Router E runs BGP and OSPF. Router F runs BGP and OSPF. Router B has a dashed line connecting it to router C, indicating they are not directly connected. Router B has solid lines connecting it to routers A, D, and E. Router D has solid lines connecting it to routers B, C, and F. Router E has solid lines connecting it to routers B, D, and F. Router F has solid lines connecting it to routers D and E. Router A has a solid line connecting it to router B. Router C has a solid line connecting it to router D. Router F has a solid line connecting it to router D. Router F has a solid line connecting it to router E. Router B has a double-headed arrow labeled "Redistributing BGP into OSPF" pointing to router C. Router B also has a double-headed arrow labeled "Redistributing BGP into OSPF" pointing to router E.

A transit AS should run IBGP on all routers because the full Internet routing table is too large to redistribute using an IGP.

Interior routing protocols, such as RIP and OSPF, form adjacency relationships with directly connected neighbors. With RIP, a router sends an update to all directly connected neighbors, who in turn advertise these routes to their directly attached neighbors. OSPF has a formal adjacency relationship. When a change occurs on an OSPF router, that router sends the update to all directly connected routers with which it has a full adjacency. Those routers flood the change to all their adjacent neighbors.

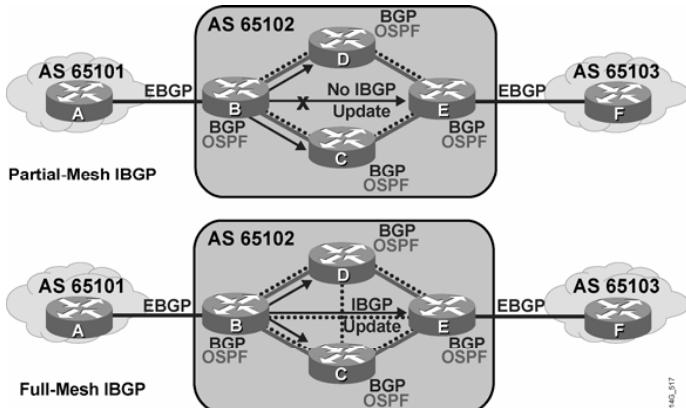
RIP, OSPF, and EIGRP use broadcast or multicast sessions to propagate changes across an AS. All routers along the pathway need to use the same protocol to be able to handle the routing updates. With an IGP, all routers need to have the same information. In an OSPF area, if one OSPF router has a 32-MB routing table, all OSPF routers in that area need to have the same 32-MB table.

As illustrated in the figure, BGP was originally intended to run along the borders of an AS with the routers in the middle of the AS ignorant of the details of BGP (hence the name “Border Gateway Protocol”). A transit AS, such as the one in the figure, is an AS that routes traffic from one external AS to another external AS. Typically, transit autonomous systems are ISPs. All routers in a transit AS must have complete knowledge of external routes. Theoretically, one way to achieve this goal is to redistribute BGP routes using an IGP at the edge routers. However, this approach has problems.

Because the current Internet routing table is very large, redistributing all the BGP routes using an IGP is not a scalable method for the interior routers within an AS to learn about the external networks. Another method that you can use is to run full-mesh IBGP within the AS.

IBGP Split Horizon Rule

Cisco.com



By default, routes learned via IBGP are never propagated to other IBGP peers.

BGP does not work in the same manner as IGPs. Because the designers of BGP could not guarantee that an AS would run BGP on all routers, a method had to be developed to ensure that IBGP speakers could pass updates to one another.

The **neighbor** command enables BGP updates between BGP speakers. Each BGP speaker is assumed to have a neighbor statement for each IBGP speaker. This neighbor statement is the required default behavior of IBGP.

The main reason that an AS needs to fully mesh its IBGP neighbors is to prevent routing loops or routing “black holes.” A rule governing IBGP behavior is the BGP split horizon rule. To avoid routing loops within an AS, the BGP split horizon rule specifies that routes learned via IBGP are never propagated to other IBGP peers.

By fully meshing all IBGP neighbors, when a change is received from an external AS, the BGP router for the local AS is responsible for informing all other IBGP neighbors of the change. IBGP neighbors that receive this update do not send it to any other IBGP neighbor, because they assume the sending IBGP neighbor is fully meshed with all other IBGP speakers and has sent each IBGP neighbor the update.

If the sending IBGP neighbor is not fully meshed with each IBGP router, the routers that are not peering with this router will have different IP routing tables than the routers that are peering with it.

The inconsistent routing tables can cause routing loops or routing black holes, because the default assumption by all routers running BGP within an AS is that each BGP router is exchanging IBGP information directly with all other BGP routers in the AS.

In the figure, the top portion shows IBGP update behavior in a partially meshed neighbor environment. Router B receives a BGP update from router A.

Router B has two IBGP neighbors, routers C and D, but does not have an IBGP neighbor relationship with router E. Routers C and D learn about any networks that were added or withdrawn behind router B. Even if routers C and D have IBGP neighbor sessions with router E, because of the BGP split horizon rule, they assume that the AS is fully meshed for IBGP and do not replicate the update and send it to router E.

Sending an IBGP update to router E is the responsibility of router B because it is the router with first-hand knowledge of the networks in and beyond AS 65101. Router E does not learn of any networks through router B and will not use router B to reach any networks in AS 65101 or other autonomous systems behind AS 65101.

In the bottom portion of the figure, IBGP is fully meshed, so when an IBGP neighbor learns of a change from an EBGP neighbor, that router is responsible for sending the update to all the other IBGP speakers in the AS.

The update is sent once to each neighbor and not duplicated by any other IBGP neighbor, which reduces unnecessary traffic. In fully meshed IBGP, each router assumes that every other internal router has a neighbor statement that points to each IBGP neighbor.

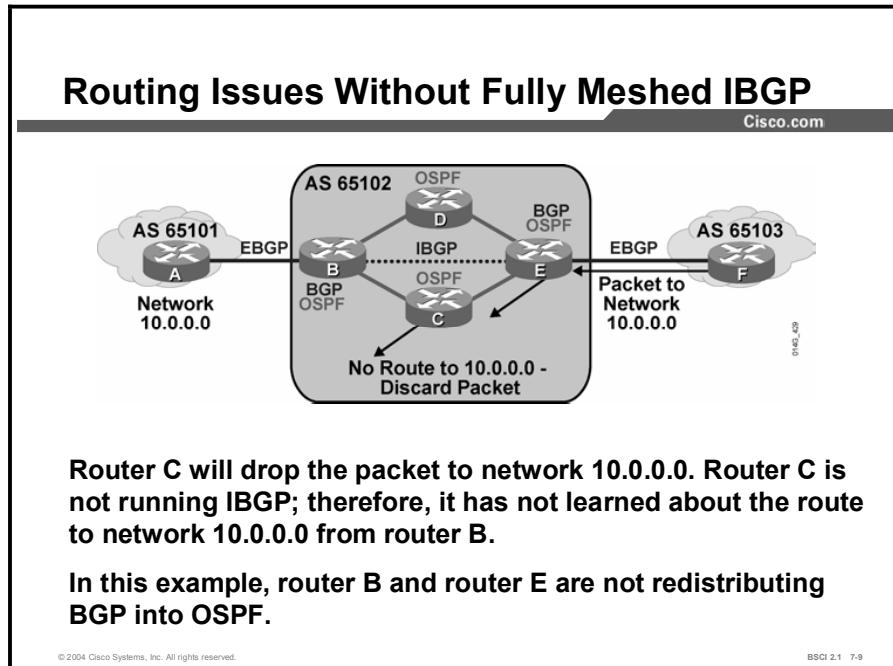
TCP was selected as the transport layer for BGP because TCP can move a large volume of data reliably. With the full Internet routing table exceeding 32 MB in size and exceeding 1000 bytes of BGP changes per minute, using TCP for windowing and reliability, as opposed to developing a BGP one-for-one windowing capability like OSPF or EIGRP, was the best solution.

TCP sessions cannot be multicast or broadcast because TCP has to ensure the delivery of packets to each recipient. Because TCP cannot use broadcasting, BGP cannot use it either, so BGP has to use fully meshed TCP sessions.

Each IBGP neighbor needs to know all the other IBGP neighbors in the same AS so that it can have a complete picture of how to exit the AS. Because all routers running BGP in an AS are fully meshed and have the same database as a result of a consistent routing policy, they can apply the same path selection formula.

The path selection results will therefore be uniform across the AS. Uniform path selection across the AS means no routing loops and a consistent policy for exiting and entering the AS.

Example



For example, in the diagram here, routers A, B, E, and F are the only ones running BGP. Router B has an EBGP neighbor statement for router A and an IBGP neighbor statement for router E. Router E has an EBGP neighbor statement for router F and an IBGP neighbor statement for router B. Routers C and D are not running BGP. Routers B, C, D, and E are running OSPF as their IGP.

Network 10.0.0.0 is owned by AS 65101 and is advertised to router B via an EBGP session. Router B advertises it to router E via an IBGP session. Routers C and D never learn about this network because it is not redistributed into the local routing protocol and routers C and D are not running BGP. If router E advertises this network to router F in AS 65103, and router F starts forwarding packets to network 10.0.0.0 through AS 65102, where would router E send the packets to reach router B?

If router E forwards packets with a destination address of 10.1.1.1 to either routers C or D, those routers do not have an entry in their routing table for network 10.0.0.0 and discard the packet.

If routers C and D have a default route going to the exit points of the AS (routers B and E), there is a good chance that if router E sends a packet for network 10.0.0.0 to routers C or D, those routers may send it back to router E, which forwards it again to routers C or D, causing a routing loop to occur. If BGP is fully meshed and routers C and D are aware of network 10.0.0.0 from router B, this problem does not occur.

In the figure, AS 65102 is responsible for moving packets between AS 65101 and AS 65103, much as an ISP would. AS 65102, or any ISP network, is a transit AS. A transit AS is responsible for passing packets from one AS to another.

Many autonomous systems have multiple connections to the Internet but do not use their bandwidth to transport packets of other autonomous systems. Autonomous systems that do not allow transit to other autonomous systems are called “stub autonomous systems.”

Most autonomous systems that are connected to the Internet are stub autonomous systems. You can enter them to purchase services or products from their web pages but cannot move through them to other autonomous systems.

Large e-commerce companies can have connections to 10 or more ISPs; however, they are in business to sell a product and not to provide transport between autonomous systems. The function of an ISP, however, is to provide this transport.

You must thus configure an ISP as a transit AS. In the figure, AS 65102 needs to run BGP on all its routers and fully mesh the IBGP session so that packets transiting AS 65102 are able to reach networks and other autonomous systems on the other side of this AS.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The key terms to describe relationships between routers running BGP are as follows:**
 - BGP speaker, or BGP router
 - BGP peer, or neighbor
 - Internal BGP (IBGP) and External BGP (EBGP)
- **EBGP neighbors are directly connected routers in different autonomous systems.**
- **IBGP neighbors are directly connected routers in the same AS that are reachable by static routes or a dynamic internal routing protocol.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-10

References

For additional information, refer to these resources:

- RFCs 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, and 2439

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 terms refer to routers that are configured to exchange BGP information with one another? (Choose two.)
- A) BGP peer
 - B) BGP speaker
 - C) BGP router
 - D) BGP neighbor
- Q2) By default, what are two conditions for status as EBGP neighbors? (Choose two.)
- A) directly connected
 - B) in the same AS
 - C) in different autonomous systems
 - D) running an IGP between them to establish an adjacency
- Q3) What are three ways to form an adjacency between IBGP neighbors by default? (Choose three.)
- A) The neighbors can be directly connected.
 - B) The neighbors can be reachable from one another by static routes.
 - C) The neighbors can be reachable from one another by a dynamic internal routing protocol.
 - D) The neighbors can be in different autonomous systems.
- Q4) What is the BGP split horizon rule?
- A) BGP must use fully meshed IBGP neighbors because TCP does not support multicast or broadcast sessions.
 - B) All the routers between IBGP neighbors may not be running BGP.
 - C) By fully meshing all IBGP neighbors, when you receive a change from an external AS, the receiving BGP router for this AS is responsible for informing all other IBGP neighbors of the change. IBGP neighbors receiving this update do not send it to any other IBGP neighbor because they assume that the sending IBGP neighbor is fully meshed with all other IBGP speakers and has sent each IBGP neighbor the update.
 - D) Other IBGP neighbors learn about the state of a given network directly from the routers that are the exit points from this AS. Thus, it is a more authoritative update than a flooding mechanism.

Quiz Answer Key

Q1) A, D

Relates to: Terminology for BGP Neighbor Relationships

Q2) A, C

Relates to: External BGP Neighbors

Q3) A, B, C

Relates to: Internal BGP Neighbors

Q4) C

Relates to: Full Mesh of IBGP Neighbors

Basic BGP Operations

Overview

This lesson presents the commands to properly configure BGP for a scalable internetwork so that it will do the following:

- Include the commands to establish a neighbor relationship
- Set the next-hop address
- Set the source IP address of a BGP update
- Announce networks to other BGP routers

This lesson also presents the various neighbor states through which BGP progresses to establish a BGP session, and tips for troubleshooting BGP if the session is stuck in the active or idle state. It also shows how to use the **show** and **debug** commands for troubleshooting BGP.

Relevance

This lesson presents how to configure and troubleshoot BGP. You must have a thorough understanding of this material in order to use BGP.

Objectives

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

- Describe basic BGP operations
- Identify BGP neighbor states
- Use BGP **show**, **debug**, and **clear** commands

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Basic BGP Configuration**
- **BGP Neighbor States**
- **BGP show, debug, and clear Commands**
- **Summary**
- **Quiz**

Basic BGP Configuration

This topic discusses the commands that are used to configure BGP features.

BGP Commands

Cisco.com

```
Router(config)#  
router bgp autonomous-system
```

- This command, with no subcommands, does not activate BGP.
- Only one instance of BGP can be configured on the router at a single time.
- The autonomous system number identifies the autonomous system to which the router belongs.
- The autonomous system number in this command is compared to the autonomous system numbers listed in neighbor statements to determine if the neighbor is an internal or external neighbor.

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 7-4

The syntax of basic BGP configuration commands is similar to the syntax for configuring internal routing protocols.

Use the **router bgp** command to identify to the router that any subsequent subcommands belong to this routing process. This command also identifies the local AS in which this router belongs. The router needs to be informed of the AS so it can determine if the BGP neighbors to be configured next are either IBGP or EBGP neighbors.

Table 1: The router bgp Command Parameters

Parameters	Description
autonomous-system	Identifies the local AS number.

The **route bgp** command alone cannot activate BGP on a router. You must enter at least one subcommand under the **router bgp** command to activate the BGP process on the router.

If you place your router in AS “A” and then try to configure a new **router bgp** “B” command, the router informs you that you are currently configured for AS A. You must insert the AS number in the **router bgp** command so that the router can properly identify the relationship between the neighboring router and itself.

The Internet Assigned Numbers Authority (IANA) is the organization responsible for allocating AS numbers. Specifically, the American Registry for Internet Numbers (ARIN) has the jurisdiction for assigning numbers for the Americas, the Caribbean, and Africa. Réseaux IP Européennes Network Information Center (RIPENIC) administers AS numbers for Europe, and the Asia Pacific Network Information Center (APNIC) administers the numbers for the Asia-Pacific region.

AS numbers are 16-bit numbers ranging from 1 to 65535; RFC 1930 provides guidelines for the use of AS numbers. A range of AS numbers, 64512 through 65535, is reserved for private use, much like private IP addresses.

Note Using an IANA-assigned AS number rather than a private AS number is necessary only if your organization plans to use an EGP, such as BGP, and connect to a public network, such as the Internet.

BGP neighbor Command

Cisco.com

```
Router(config-router)#  
neighbor {ip-address | peer-group-name}  
remote-as autonomous-system
```

- The **neighbor** command activates a BGP session with this neighbor.
- The term **remote-as** shows what AS this neighbor is in. This AS number is used to determine if the neighbor is internal or external.
- This command is used for both external and internal neighbors.
- The IP address that is specified is the destination address of BGP packets going to this neighbor.
- This router must have an IP pathway to reach this neighbor before it can set up a BGP relationship.

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 7-5

You use the **neighbor ip-address remote-as autonomous-system** command to activate a BGP session for external and internal neighboring routers. The address that is used in this command is the destination address for all BGP packets going to this neighboring router. In order for BGP to pass BGP routing information, this address must be reachable.

Before you enter the **neighbor** command, verify that the address that you plan to use is reachable. This command is mandatory for the establishment of each neighboring router relationship because BGP attempts to establish a TCP session and exchange BGP updates with the device at this IP address.

The AS number that is a part of this command is used to identify if this neighbor is an EBGP neighbor or an IBGP neighbor. If the AS number is the same as the AS number for this router, that neighbor is an IBGP neighbor and the IP address listed in this **neighbor** command does not have to be directly connected. If the AS number is different from the AS number for this router, this neighbor is an EBGP neighbor and the address in this **neighbor** command must be directly connected by default.

Use the **neighbor remote-as** command to identify a peer router with which the local router will establish a session.

Table 2: The neighbor remote-as Command Parameters

Parameter	Description
<i>ip-address</i>	Identifies the peer router.
<i>peer-group-name</i>	Identifies the name of a BGP peer group.
<i>autonomous-system</i>	Identifies the AS of the peer router.

BGP shutdown Commands

Cisco.com

```
Router(config-router)#
neighbor {ip-address | peer-group-name} shutdown
```

- Administratively brings down a BGP neighbor
- Used for maintenance and policy changes to prevent route flapping

```
Router(config-router)#
no neighbor {ip-address | peer-group-name} shutdown
```

- Re-enables a BGP neighbor that has been administratively shut down

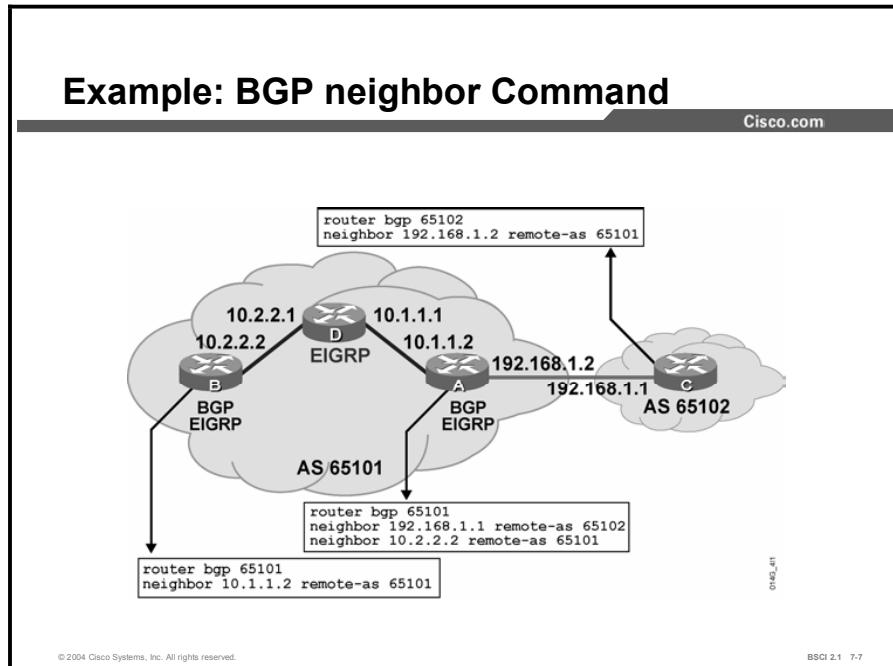
©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-6

Use the **neighbor *ip-address* shutdown** commands to administratively shut down and re-enable a BGP neighbor.

If you implement major policy changes to a neighboring router and you change multiple parameters, you must administratively shut down the neighboring router, implement the changes, and then bring the neighboring router back up with the **no neighbor *ip-address* shutdown** command.

Example



In the figure, router A in AS 65101 has two neighbor statements, and neighbor 10.2.2.2 (router B) is in the same AS as router A. These neighbor statements define router B as an IBGP neighbor. AS 65101 runs EIGRP between all internal routers.

Router A has an EIGRP pathway to reach IP address 10.2.2.2. As an IBGP neighbor, Router B can be multiple routers away from router A.

Router A knows that router C (neighbor 192.168.1.1 remote-as 65102) is an external neighbor because AS 65102 in the neighbor statement for router C does not match the AS number of router A, which is AS 65101.

Router A can reach AS 65102 via 192.168.1.1, which is directly connected to router A.

BGP Issues with Source IP Address

Cisco.com

- When you are creating a BGP packet, the neighbor statement will be the destination IP address and the outbound interface will be the source IP address.
- When a BGP packet is received for a new BGP session, the source address of the packet is compared to the list of neighbor statements.
 - If a match is found, a relationship is established.
 - If no match is found, the packet is ignored.
- Make sure that the source IP address matches the address that the other router has in its neighbor statement.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

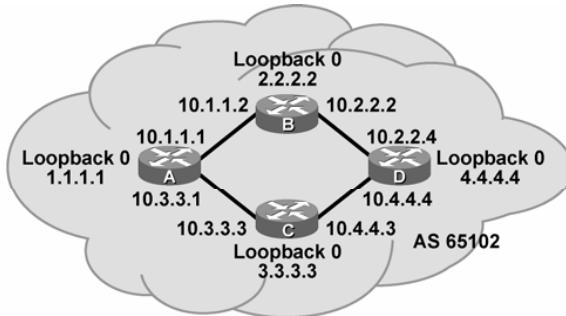
The BGP neighbor statement informs the router of the destination IP address for each update packet. The router must decide which IP address to use as the source IP address in the BGP routing update.

When a router creates a BGP packet for a neighbor, it checks the routing table for the destination network to reach that neighbor. The IP address of the outbound interface, as the routing table indicates, is used as the source IP address of the BGP packet.

This source IP address must match the address in the neighbor statement of the other router. Otherwise, you can have problems with peering in BGP because you are not able to establish the BGP session.

IBGP Peering Issue

Cisco.com



To establish the IBGP session between router A and router D, which neighbor addresses should be used?

What IP address should router A use for peering with router D? What IP address should router D use for peering with router A?

10.4.4.4
10.2.2.4
4.4.4.4

10.1.1.1
10.3.3.1
1.1.1.1

0140_412

BSCI 2.1 7-9

© 2004 Cisco Systems, Inc. All rights reserved.

To establish the IBGP session between router A and router D, as shown in this figure, which neighbor IP address should be used?

The problem is as follows: If router D uses **neighbor 10.3.3.1 remote-as 65102**, but router A is sending the BGP packets to router D via router B, the source IP address will be 10.1.1.1.

When router D receives this BGP packet via router B, it will not recognize this BGP packet because 10.1.1.1 was not configured as a neighbor of router D. Therefore, the IBGP session between router A and router D cannot be established.

A solution to this problem is to establish the IBGP session using a loopback interface when there are multiple paths between the IBGP neighbors.

BGP Neighbor Update Source Address

Cisco.com

```
Router(config-router)#
neighbor {ip-address | peer-group-name} update-source
interface-type interface-number
```

- This command allows the BGP process to use the IP address of a specified interface as the source IP address of all BGP updates to that neighbor.
- A loopback interface is usually used, because it will be available as long as the router is operational.
- The IP address used in this command will be the destination IP address of all BGP updates and should be the loopback interface of the other router.
- The update-source command is normally used only with IBGP neighbors.
- The address of an EBGP neighbor must be directly connected by default. The loopback of an EBGP neighbor is not directly connected.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-10

The **update-source** option in the **neighbor** command overrides the default source IP address that you use for BGP packets. It is necessary to tell the router which IP address to use as the source address for all BGP packets when you use a loopback address.

If you do not use the **update-source** option in the **neighbor** command, an announcement going to a neighbor uses the IP address of the exiting interface as the source address for a packet. When a router creates a packet, whether it is a routing update, a ping, or any other type of IP packet, the router does a lookup in the routing table for the destination address.

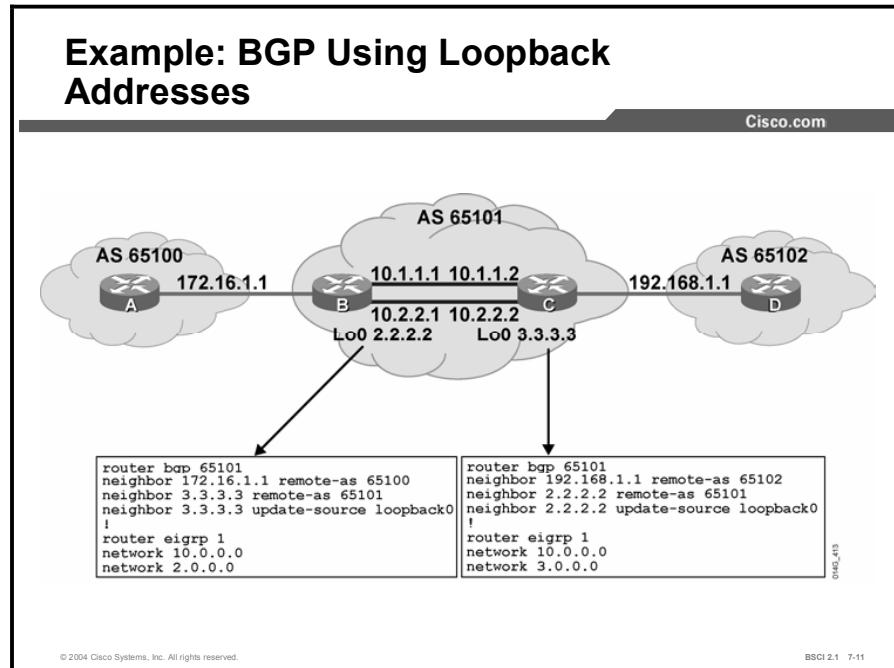
The routing table lists the appropriate interface to get to the destination address. The address of this outbound interface is used as the source address of that packet by default.

The neighboring router that receives the update packet looks at the source address of the packet and sees that it has no neighbor relationship with that source address; it then discards this packet.

The receiving router discards this packet because the receiving router points at the loopback address of the sender in its neighbor statement. The receiving router does not recognize the current sender because it does not have a relationship with the source IP address of the current packet.

BGP does not accept unsolicited updates; it must be aware of every neighboring router and have a neighbor statement for it.

Example



In the figure shown here, router B has router A as an EBGP neighbor. The only reachable address for router B to use for a neighbor address in BGP is the directly connected address of 172.16.1.1. Router B has multiple pathways to reach router C, an IBGP neighbor.

All networks, including the IP network for the loopback interface of router C, can be reached from router B. Router B can reach these networks because routers B and C exchange EIGRP updates; router B and router A do not exchange updates.

The neighbor relationship is not tied to a physical interface because router B peers with the loopback interface on router C and uses its loopback address as the source IP address. If router B peers with 10.1.1.2 on router C and that interface goes down, the BGP neighbor relationship cannot be established.

The routers are not tied to physical interfaces for connectivity because router B points at the loopback address of router C and vice versa, using the loopback address as the source IP address for the update packet.

Multiple pathways can exist to reach each neighbor when you peer with IBGP neighboring routers. If the BGP router is using a neighbor address, which is assigned to a specific interface on another router, and that interface goes down on the other router, the router pointing at this address loses its BGP session with that neighbor.

If the router peers with the loopback interface of the other router, the loopback interface will always be available as long as the router itself does not fail.

This peering arrangement adds resiliency to the IBGP sessions because the routers are not tied into a physical interface, which may go down for any number of reasons.

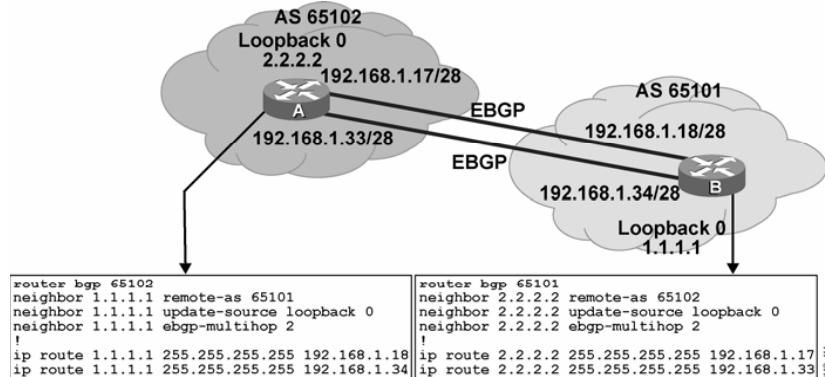
To peer with the loopback of another internal neighbor, the first router would point the neighbor statement at the loopback address of the other internal neighbor. Ensure that both routers have a route to the loopback address of the other neighbor in their routing table. Also ensure that both routers are announcing their loopback addresses into their local routing protocol.

The **neighbor update-source** command is necessary for both routers. If router B points at loopback address 3.3.3.3 of router C, and router C points at loopback address 2.2.2.2 of router B, and neither uses the **neighbor update-source** command, there are issues with starting a BGP session between these routers.

Without this command, router B sends a BGP open packet to router C with the source IP address being either 10.1.1.1 or 10.2.2.1. Router C reviews the source IP address and attempts to match it against its list of known neighbors. Router C does not find a match and does not respond to the open message from router B.

Example: **ebgp-multihop** Command

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-12

When an EBGP router is peering with an external neighbor, the only address that it can reach without further configuration is the interface that is directly connected to that EBGP router. Because you do not pass internal routing information with external peers, you have to point to a directly connected address for that external neighbor.

The loopback is never directly connected. To reach the loopback, you have to use static routes pointing at the physical address of the directly connected network (the next-hop address). In addition to the static route, you need to make use of the **neighbor ebgp-multihop** command. This command increases the default of one hop for EBGP peers by changing the default Time to Live (TTL) value of 1. It provides you with a route to the EBGP loopback address and a hop value greater than 1. This command is of value to you when redundant paths exist between EBGP neighbors.

In the figure shown here, router A in AS 65102 has two pathways to router B in AS 65101. If router A uses a single neighbor statement and points at 192.168.1.18 on router B of AS 65101 and that link goes down, there is no BGP session between these autonomous systems. No packets pass from one AS to the next, although another link exists. If router A uses two neighbor statements pointing at 192.168.1.18 and 192.168.1.34 on router B, it partially solves the problem; however, every BGP update that router A receives is sent to router B twice because there are two neighbor statements.

As the figure shows, router A points at the loopback address of router B and vice versa, and each router uses its loopback address as the source IP address for its BGP updates. Because an IGP is not used between autonomous systems, neither router can reach the loopback of the other router without assistance. Each router needs to use two static routes to inform BGP of the pathways available to reach the loopback address of the other router. An EBGP neighbor address must be directly connected, so you must use the **neighbor ebgp-multihop** command to change the default setting of BGP and inform BGP that this neighbor IP address is more than one hop away. In the figure, the command used on router A is set to inform BGP that the neighbor address of 1.1.1.1 is two hops away.

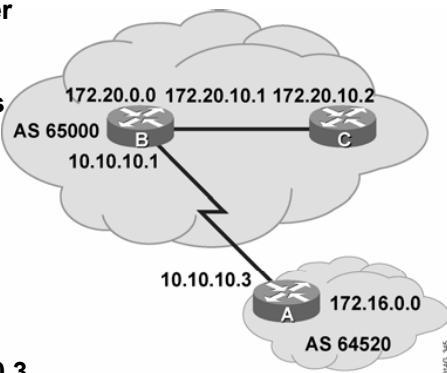
Next-Hop Behavior

Cisco.com

BGP is an AS-by-AS routing protocol, not a router-by-router routing protocol.

In BGP, the next hop does not mean the next router; it means the IP address to reach the next AS.

- Router A advertises network 172.16.0.0 to router B in EBGP, with a next hop of 10.10.10.3.
- Router B advertises 172.16.0.0 in IBGP to router C, keeping 10.10.10.3 as the next-hop address.



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-13

The way in which BGP establishes an IBGP relationship is very different from how IGPs behave. The method that BGP uses to denote its next-hop address is also very different from how an IGP performs the same function.

For EBGP, the default next hop is the IP address of the neighboring router that sent the update. In the figure, router A advertises 172.16.0.0 to router B with a next hop of 10.10.10.3. Router B advertises 172.20.0.0 to router A, with a next hop of 10.10.10.1.

For IBGP, the BGP protocol states that the next hop advertised by EBGP should be carried into IBGP. Because of this rule, router B advertises 172.16.0.0 to its IBGP peer router C with a next hop of 10.10.10.3, the address of router A. Therefore, router C knows that the next hop to reach 172.16.0.0 is 10.10.10.3.

It is very important for router C to know how to reach the 10.10.10.0 subnet, either through an IGP or a static route. Otherwise, router C drops packets destined for 172.16.0.0 because it is not able to get to the next-hop address for that network.

An IBGP neighboring router performs a recursive lookup to find out how to reach a BGP next-hop address by using its IGP entries in the routing table.

For example, router C learns in a BGP update about network 172.16.0.0/16 from a route source of 172.20.10.1, router B, and has a next hop of 10.10.10.3, router A. Router C installs the route to 172.16.0.0/16 in the routing table with a next hop of 10.10.10.3. Router B should announce network 10.10.10.0/24 using its IGP to router C. Router C installs that route into its routing table with a next hop of 172.20.10.1.

An IGP uses the source IP address of a routing update (route source) as the next-hop address. BGP uses a separate field per network to record the next-hop address. If router C has a packet to send to 172.16.100.1, it looks up the network in the routing table and finds a BGP route with a next hop of 10.10.10.3. Because it is a BGP entry, router C completes a recursive lookup in the routing table for a pathway to network 10.10.10.3. The IGP has placed a route to network

10.10.10.0 in the routing table with a next hop of 172.20.10.1. Router C then forwards the packet destined for 172.16.100.1 to 172.20.10.1.

BGP is an external routing protocol that informs the next AS about pathways to other autonomous systems and the networks that those other autonomous systems own. BGP, like IGPs, is a hop-by-hop routing protocol.

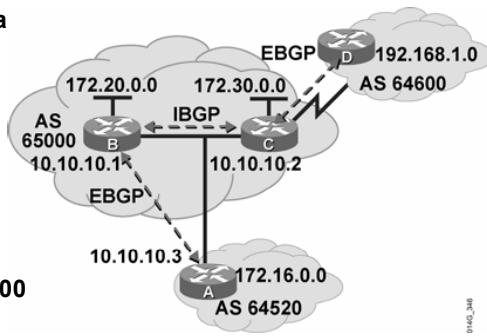
However, unlike IGPs, BGP routes from AS to AS, and the default next hop is the next AS. An IBGP neighboring router that learns about a network outside of its AS sees, as the next-hop address, the entry point for the next AS along the pathway to reach the distant network.

Next Hop on a Multiaccess Network

Cisco.com

The following takes place in a multiaccess network:

- Router B advertises network 172.30.0.0 to router A in EBGP with a next hop of 10.10.10.2, not 10.10.10.1. This avoids an unnecessary hop.
- BGP is being efficient by informing AS 64520 of the best entry point into AS 65000 for network 172.30.0.0.
- Router B in AS 65000 also advertises to AS 64520 that the best entry point for each network in AS 64600 is the next hop of router C because that is the best pathway to move through AS 65000 to AS 64600.



©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-14

0140-346

When running BGP over a multiaccess network such as Ethernet, a BGP router adjusts the next-hop address to avoid inserting additional hops into the network. This feature is sometimes called a third-party next hop.

As shown in the figure, routers B and C in AS 65000 are running an IBGP. Router B can reach network 172.30.0.0 via 10.10.10.2. Router B also runs EBGP with router A. When router B sends a BGP update to router A regarding 172.30.0.0, it uses 10.10.10.2 as the next hop and not its own IP address (10.10.10.1). Because the network between the three routers is a multiaccess network, router A uses router C as a next hop to reach 172.30.0.0.

The next-hop address issue makes more sense when you review it from an ISP perspective. A large ISP at a public peering point has multiple routers peering with different neighboring routers. It is not possible for one router to peer with every neighboring router at the major public peering points. Router B may peer with AS 64520, and router C may peer with AS 64600.

From the perspective of router A, it must have a pathway through AS 65000 to get to networks in and behind AS 64600. Router A has a neighbor relationship with only router B in AS 65000; however, router B does not handle traffic going to AS 64600.

The preferred pathway of router B to AS 64600 is through router C, 10.10.10.2. Router B must advertise the networks for AS 64600 to router A, 10.10.10.3. Router B notices that routers A and C are on the same subnet. Router B informs router A to install the AS 64600 networks with a next hop of 10.10.10.2 and not 10.10.10.1.

The next-hop-self Command

Cisco.com

```
Router(config-router)#
neighbor {ip-address | peer-group-name} next-hop-self
```

- Forces all updates for this neighbor to be advertised with this router as the next hop.
- The IP address used for next-hop-self will be the same as the source IP address of the BGP packet.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-15

It is sometimes necessary to override the default next-hop behavior of a router and force it to advertise itself as the next-hop address for routes sent to a neighboring router.

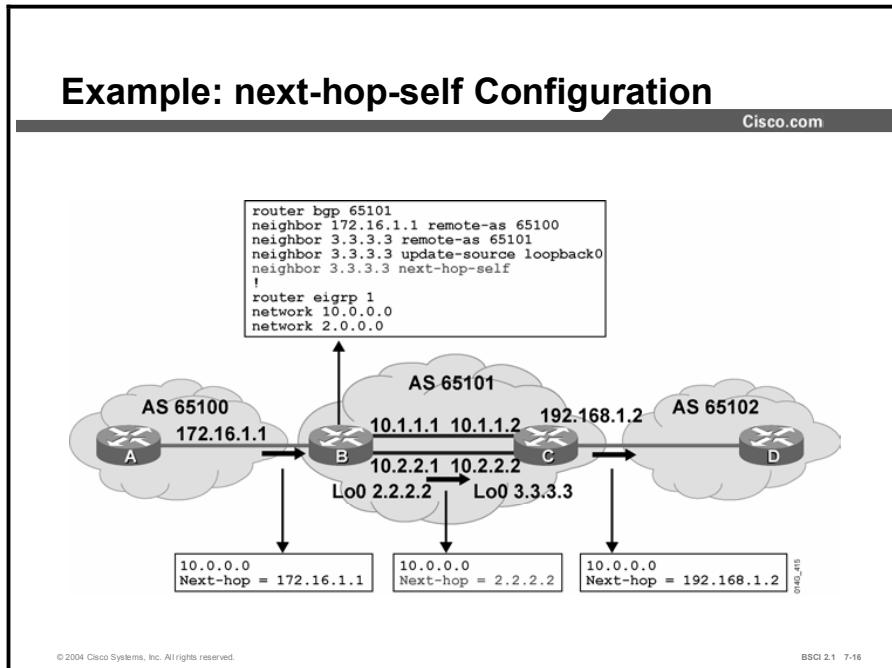
The **neighbor next-hop-self** command forces BGP to use the source IP address of itself as the update address in the next-hop address field for each network that it advertises to the neighbor address.

An internal protocol, such as RIP, EIGRP, or OSPF, always uses the source IP address of a routing update as the next-hop address for each network that is placed in the routing table. The **neighbor next-hop-self** command makes BGP use the source IP address of the update as the next-hop address for each advertised network.

Table 3: The neighbor next-hop-self Command Parameters

Parameter	Description
<i>ip-address</i>	Identifies the peer router to which advertisements are sent with this router identified as the next hop.
<i>peer-group-name</i>	Identifies the name of a BGP peer group.

Example



In the figure, router B views all routes learned from AS 65100 as having a next hop of 172.16.1.1, which is the entrance to AS 65100 for router B. When router B announces those networks to its IBGP neighbors in AS 65101, the BGP default setting is to announce that the next hop to reach each of those networks is the entrance to AS 65100 (172.16.1.1).

This is because BGP is an AS-by-AS routing protocol. For any BGP router to reach networks in or behind AS 65100, those routers need to reach network 172.16.1.1. You need to include the network that represents 172.16.1.1 in the internal routing protocol.

In this example, router B uses the **neighbor next-hop-self** command to change the default BGP settings. Once this command is given, router B advertises a next hop of 2.2.2.2 (the IP address of the loopback interface) to its IBGP neighbor, because that is the source IP address of the routing update to its IBGP neighbor.

When router C announces networks that are in or behind AS 65101 to EBGP neighbors, such as router D in AS 65102, router C uses its outbound interface address as the next-hop address.

The default source IP address for router C for this neighbor is its outbound interface of 192.168.1.2. This address is also the default next-hop address for router D to use to reach any networks in or behind AS 65101.

Peer Groups

Cisco.com

```
Router(config-router)#
```

```
neighbor [peer-group-name] peer-group
```

- Creates peer group

```
Router(config-router)#
```

```
neighbor [ip-address] peer-group [peer-group-name]
```

- Defines a template with parameters set for a group of neighbors instead of individually
- Useful when many neighbors have the same outbound policies
- Members can have a different inbound policy
- Updates generated once per peer group
- Simplifies configuration

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-17

In BGP, neighboring routers are often configured with the same update policies. For example, the neighboring routers may have the same filtering applied. On Cisco routers, neighboring routers with the same update policies can be grouped into peer groups to simplify configuration and to make updating more efficient. For configurations with many peers, this approach is highly recommended.

A BGP peer group is a group of BGP neighboring routers with the same update policies.

Members of the peer group inherit all the configuration options of the peer group. You can configure members to override these options if these options affect inbound advertisements and not outbound ones.

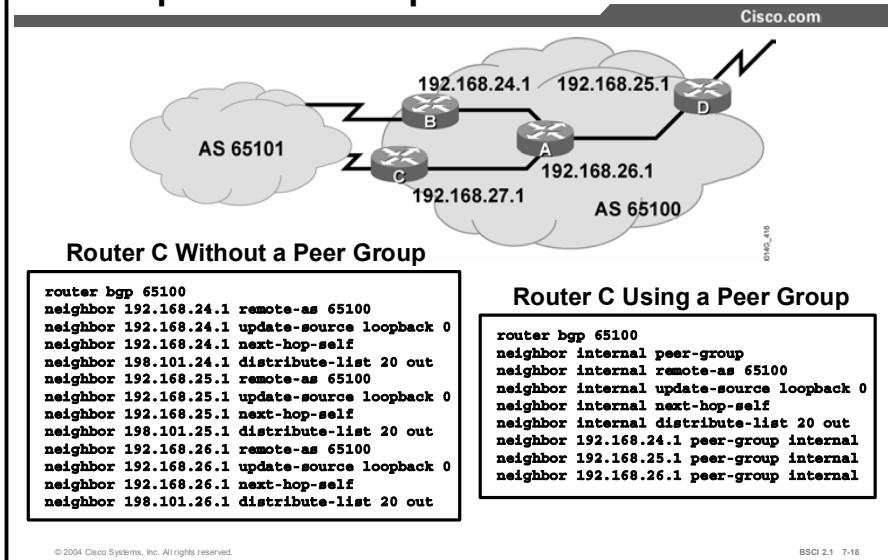
Peer groups are more efficient because updates are generated only once per peer group rather than once for each neighboring router. The peer group name is local to the router on which it is configured, and it is not passed to any other router. Peer groups make the router configuration easier to read and improve the performance of the router. Without a peer group, a router creates separate updates for each neighboring router, although those neighbors may have an identical outbound policy. With a peer group, the router creates one update for the peer group and then duplicates it for each member.

Use the following command to create a peer group and define the name for linking similar neighboring routers together. This command applies a consistent policy to all the neighboring routers:

```
neighbor peer-group-name peer-group
```

Use the second command in the figure, **neighbor [ip-address] peer-group [peer-group-name]**, to link the address of a neighboring router to a specific peer group name. A neighboring router can be part of only one peer group. This command allows you to type in the peer group name instead of typing in the IP address to link the policy to the neighboring router. You must enter the **neighbor peer-group-name peer-group** command before the router will accept the second command.

Example: Peer Group



In the figure, AS 65100 has four routers running IBGP. All these IBGP neighbors are peering with the loopback 0 interface of each other and are using the IP address of their loopback 0 interface as the source IP address for all BGP packets. Each router is using one of its own IP addresses as the next-hop address for each network advertised through BGP. These are outbound policies.

In addition, router C has an outbound distribution list associated with each IBGP neighbor. This outbound filter performs the same function as the **distribute-list** command that you use for internal routing protocols; however, it is linked to a specific neighbor for use with BGP. The ISP behind router C may be announcing RFC 1918 private address space to router C. Router C does not want to pass these networks to other routers running BGP in AS 65100.

To accomplish this goal, access list 20 might look like the following:

```
access-list 20 deny 10.0.0.0 0.255.255.255
access-list 20 deny 172.16.0.0 0.31.255.255
access-list 20 deny 192.168.0.0 0.0.255.255
access-list 20 permit any
```

The figure shows the output for router C when the router is not using a peer group. All IBGP neighbors have the outbound distribute list link to them individually. If router C receives a change from AS 65101, router C must generate an individual update for each IBGP neighbor and run each update against distribute list 20. If router C has a large number of IBGP neighbors, the processing power needed to inform the IBGP neighbors of the changes in AS 65101 could be extensive.

The figure also shows the output for router C when it is using a peer group called “internal.” The **update-source**, **next-hop-self**, and **distribute-list 20 out** commands are all linked to peer group internal, which in turn is linked to each of the IBGP neighbors. If router C receives a

change from AS 65101, router C creates a single update and processes it through distribute list 20 once. The update is replicated for each neighbor that is part of the internal peer group. This action saves processing time in generating the updates for all IBGP neighbors.

Thus, the use of peer groups can improve efficiency when processing updates for BGP neighbors that have a common outbound BGP policy.

Adding a new neighbor to router C using a peer group with the same policies of the other IBGP neighbors requires adding only a single neighbor statement to link the new neighbor to the peer group internal. Adding that same neighbor to router C without a peer group requires four neighbor statements.

Using a peer group also makes the configuration easier to read and to change. If you need to add a new policy, such as a route map, to all IBGP neighbors on router C using a peer group, you need only to link the route map to peer group internal. For router C without a peer group, you need to add the new policy to each neighbor.

BGP network Command

Cisco.com

```
Router(config-router)#  
network network-number [mask network-mask]
```

- This command tells BGP what network to advertise, not how to advertise the network.
- The command does not activate the protocol on an interface.
- Without a mask option, the command advertises classful networks. If a subnet of the classful network exists in a routing table, the classful address is announced if autosummary is enabled. Autosummary is enabled by default.
- BGP looks for an exact match in the local routing table before announcing this route.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-19

Use the **network** command to permit BGP to advertise a network if it is present in the IP routing table.

Table 4: The network Command Parameters

Parameter	Description
network-number	Identifies an IP network to be advertised by BGP.
network-mask	(Optional) Identifies the subnet mask to be advertised by BGP.

The **network** command determines which networks that the router originates. This concept is different from using the **network** command when you are configuring an IGP. Unlike an IGP, the **network** command does not start up BGP on specific interfaces; rather, it indicates to BGP which networks it should originate from this router.

Use the **mask** parameter because BGP4 can handle subnetting and supernetting. The list of **network** commands must include all networks in the AS that you want to advertise, not just those that are locally connected to the router.

Prior to Cisco IOS software Release 12.0, there was a limit of 200 **network** commands per BGP router. This limit has been removed. The resources of the router, such as the configured NVRAM or RAM, determine the maximum number of **network** commands that you can use.

The command **network network-number** allows BGP to advertise an IGP route if it is already in the IP routing table. The **neighbor** command tells BGP where to advertise. The **network** command tells BGP what to advertise.

The sole purpose of the **network** command is to notify BGP of which network to advertise. Without using the mask modifier, this command announces only the classful network number.

At least one subnet of the specified major network must be present in the IP routing table to allow BGP to start announcing the classful network as a BGP route. However, if you disable autosummary, an exact match to the network must exist in the routing table. Before BGP announces a route, it checks to see if it can reach it.

For example, if you misconfigure a network statement like network 198.1.1.1 mask 255.255.255.0, BGP looks for 198.1.1.1/24 in the routing table. It may find 198.1.1.0/24 or 198.1.1.1/32; however it never finds 198.1.1.1/24. Because the routing table does not contain a specific match to the network, BGP does not announce the 198.1.1.1/24 network to any neighbors.

If you specify a statement like network 198.1.0.0 mask 255.255.0.0 to advertise a CIDR block, BGP looks for 198.1.0.0/16 in the routing table. It may find 198.1.1.0/24 or 198.1.1.1/32; however, it never finds 198.1.0.0/16.

Because the routing table does not contain a specific match to the network, BGP does not announce the 198.1.0.0/16 network to any neighbors. In this case, you can configure the following static route toward the null interface so BGP can find an exact match in the routing table.

After finding an exact match in the routing table, BGP announces the 198.1.0.0/16 network to any neighbors:

```
ip route 198.1.0.0 255.255.0.0 null0
```

BGP Synchronization

Cisco.com

Synchronization rule: Do not use or advertise to an external neighbor a route learned by IBGP until a matching route has been learned from an IGP.

- Ensures consistency of information throughout the AS
- Avoids black holes within the AS
- Safe to turn off if all routers in the AS are running full-mesh IBGP

```
Router(config-router)#  
no synchronization
```

- **Disables BGP synchronization so that a router will advertise routes in BGP without learning them in IGP**

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-28

The BGP synchronization rule states that a BGP router should not use or advertise to an external neighbor a route that is learned from IBGP unless that route is local or the router learns it from the IGP. If an AS passes traffic to another AS, BGP should not advertise a route before all routers in the AS have learned about the route via the IGP (by redistributing BGP into the IGP).

A router learning a route via IBGP waits until the IGP has propagated the route within the AS and then advertises it to external peers. This rule ensures that all routers in the AS are synchronized and are able to route traffic that the AS advertises to other autonomous systems.

This approach ensures consistency of routing information (avoids “black holes”) within the AS. BGP synchronization is enabled by default. It is safe to turn off BGP synchronization if all routers within the AS are running full-mesh IBGP.

Before BGP can place networks that it learned through an IBGP neighbor in the IP routing table, the route must be in the local routing table. BGP and the IGP must be synchronized before the networks learned from an IBGP neighbor can be used.

If you use the **no synchronization** command to disable the synchronization, BGP can use networks learned from an IBGP neighbor that are not present in the local routing table.

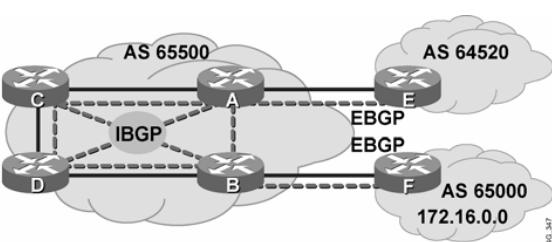
BGP synchronization is unnecessary in some situations. If all routers in your AS are running IBGP, you can disable synchronization. Disabling the synchronization feature allows you to carry fewer routes in your IGP and allows BGP to converge more quickly.

Use synchronization if there are routers in the AS that are not running BGP; therefore, the routers do not have full-mesh IBGP within the AS.

Example: BGP Synchronization

Cisco.com

- All routers in AS 65500 are running BGP; there are no matching IGP routes.



- If synchronization is on (the default), then:

- Routers A, C, and D would not use or advertise the route to 172.16.0.0 until they receive the matching route via an IGP.
- Router E would not hear about 172.16.0.0.

- If synchronization is off, then:

- Routers A, C, and D would use and advertise the route that they receive via IBGP; router E would hear about 172.16.0.0.
- If router E sends traffic for 172.16.0.0, routers A, C, and D would route the packets correctly to router B.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-21

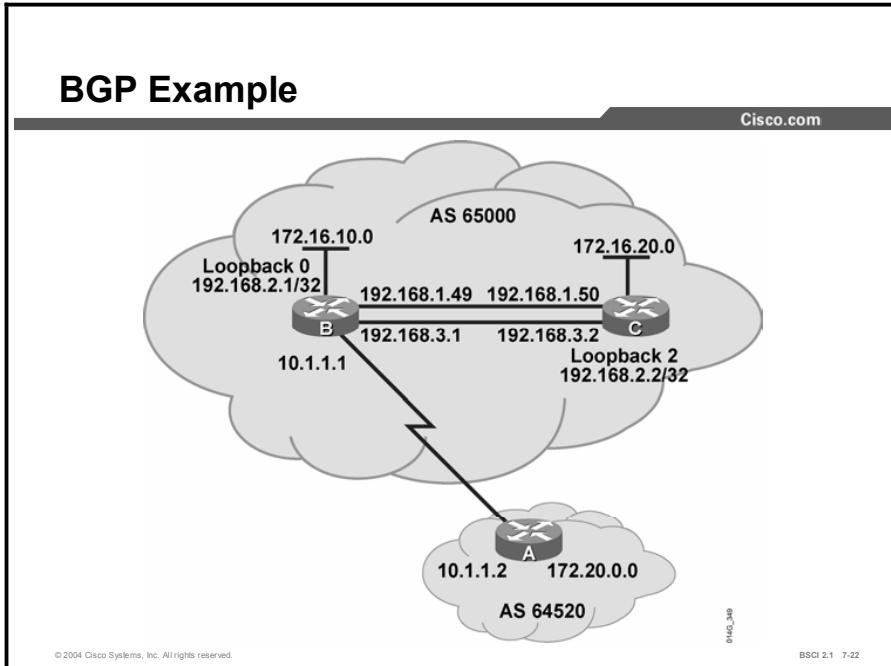
The synchronization rule results in other behavior on BGP routers.

In the figure, routers A, B, C, and D are all running IBGP and the IGP with each other. There are no matching IGP routes for the BGP routes (routers A and B are not redistributing the BGP routers into the IGP). Routers A, B, C, and D have IGP routes to the internal networks of AS 65500 but do not have routes to external networks like 172.16.0.0.

Router B advertises the route to 172.16.0.0 to the other routers in AS 65500 using IBGP. By default (with synchronization on), routers A, C, and D do not use the route to 172.16.0.0, nor does router A advertise that route to router E in AS 64520. Router B uses the route to 172.16.0.0 and installs it in its routing table. If router E receives traffic that is destined for network 172.16.0.0, it does not have a route for that network and cannot forward the traffic.

If synchronization is turned off in AS 65500, routers A, C, and D can use the route to 172.16.0.0 and install the route in their routing tables even if there are no matching IGP routes for the BGP routes. Router A advertises the route to router E. Router E then has a route to 172.16.0.0 and may send traffic that is destined for that network. Router E sends the packets to router A, and router A forwards them to router C. Router C learns a route to 172.16.0.0 via IBGP; therefore, router C forwards the packets to router D. Router D forwards the packets to router B. Router B forwards the packets to router F for network 172.16.0.0.

In modern autonomous systems, because the size of the Internet routing table is large, redistributing from BGP into an IGP is not scalable; therefore, most modern autonomous systems run full-mesh IBGP and disable synchronization. Advanced BGP configuration methods, for example, using route reflectors and confederations, reduce the full-mesh requirements.



This figure shows another BGP example. The configuration for router B follows.

BGP Example Configuration

Cisco.com

```
1. RouterB(config)# router bgp 65000
2. RouterB(config-router)# neighbor 10.1.1.2 remote-as 64520
3. RouterB(config-router)# neighbor 192.168.2.2 remote-as 65000
4. RouterB(config-router)# neighbor 192.168.2.2 update-source loopback 0
5. RouterB(config-router)# neighbor 192.168.2.2 next-hop-self
6. RouterB(config-router)# network 172.16.10.0 mask 255.255.255.0
7. RouterB(config-router)# network 192.168.1.0
8. RouterB(config-router)# network 192.168.3.0
9. RouterB(config-router)# no synchronization
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-23

This figure shows the configuration for router B. The first two commands under the **router bgp 65000** command establish that router B has the following two BGP neighbors:

- Router A in AS 64520
- Router C in AS 65000

From the perspective of router B, router A is an EBGP neighbor and router C is an IBGP neighbor.

The neighbor statement of router B to router A is pointing at the directly connected IP address to reach the EBGP neighbor, router A. Router B points at the loopback interface of router C in the neighbor statement. Router B has multiple pathways to reach router C.

If router B points at the 192.168.3.2 IP address of router C and that interface goes down, router B is unable to re-establish the BGP session until the link comes back up. If router B points at the loopback interface of router C, the link stays established as long as any pathway to router C is available. Router C should also point at the loopback address of router B in its configuration.

Line 4 notifies router B to always use its loopback 0 address, 192.168.2.1, as the source IP address when sending an update to router C, 192.168.2.2. This address is the IP address of the loopback 2 interface of router C.

In line 5, router B advertises the networks that are reachable through it. The default next-hop setting for networks from AS 64520 is IP address 10.1.1.2. With the **next-hop-self** command, router B advertises to router C a next-hop address of the loopback 0 address of router B. This command sets the next-hop address to the source IP address of the routing update. The **update-source** command sets the source IP address to the loopback 0 interface of router B.

Lines 6 and 7 notify BGP of what networks to advertise. Line 6 contains a subnet of a class B address. To announce this subnet, use the **mask** option. Lines 7 and 8 have two network

statements for the two class C networks that connect router B and router C. The default mask is 255.255.255.0, and you do not need to include it.

In line 9, synchronization is turned off. If router A is advertising 172.20.0.0 in BGP, router B receives that route and advertises it to router C. Router C cannot use this route unless it has synchronization turned off.

If router C had EBGP neighbors of its own and router B wanted to use router C as the pathway to those networks, router B would also need to turn synchronization off. Synchronization can be disabled because all the routers within the AS are running IBGP.

BGP Neighbor States

This topic discusses the states of a BGP peering relationship. The topic also discusses how to troubleshoot a BGP session using the **show** and **debug** commands.

BGP States

Cisco.com

When establishing a BGP session, BGP goes through the following steps:

- 1. Idle:** Router is searching routing table to see if a route exists to reach the neighbor.
- 2. Connect:** Router found route and has completed three-way TCP handshake.
- 3. Open sent:** Open message sent with the parameters for the BGP session.
- 4. Open confirm:** Router received agreement on the parameters for establishing session.
- 5. Established:** Peering is established; routing begins.

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-24

After the TCP handshake is complete, the BGP application tries to set up a session with the neighbor. A number of steps must occur for the session to establish itself.

Once you have entered the **neighbor** command in BGP, BGP takes the IP address that is listed and checks the local routing table for a route to this address. At this point, BGP is in an idle state. If BGP does not find a route to the IP address, it stays in the idle state. If it finds a route, it goes to the connect state when the TCP handshaking synchronize acknowledge (SYN ACK) packet returns.

After the TCP connection has finished, BGP creates a BGP open packet and sends it out. Once BGP dispatches this open packet, the BGP peering session changes to the “open sent” state. After no response for 5 seconds, the state changes to the active state.

If a response does come back in a timely manner, BGP goes to the “open confirm” state and starts scanning (evaluating) the routing table for the pathways to send to the neighbor. When those pathways have been found, BGP then goes to the established state and begins routing between the neighbors.

BGP Session Establishment

Cisco.com

The best way to see session setup is with the following command:

```
RouterA#  
debug ip bgp events
```

```
RouterA#  
BGP : 172.16.1.2 passive open  
BGP : 172.16.1.2 went from idle to connect  
BGP : 172.16.1.2 open rcvd, version 4  
BGP : 172.16.1.2 went from connect to open sent  
BGP : 172.16.1.2 sending open, version 4  
BGP : 172.16.1.2 went from open sent to open confirm  
BGP : Scanning routing tables  
BGP : 172.16.1.2 went from open confirm to established
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-25

Use the **debug ip bgp events** command to view BGP handshaking for neighbor establishment. In the figure, notice that BGP does not go into the active state because it received the open confirm message from its neighbor in a timely manner.

BGP is trying to set up the session with a neighbor at address 172.16.1.2. The 172.16.1.2 address is the address in the neighbor statement under the BGP process for this router.

In the first line of the debug, BGP is in a passive open state, which means it is looking for the address (172.16.1.2) in the routing table. The BGP state at this point is idle.

The second line indicates that the BGP process has found a route to 172.16.1.2 in the routing table and is now performing the TCP handshake with that neighbor. This line also shows the BGP state changing from idle to connect.

The third line signifies that this router has received an open message from 172.16.1.2.

The fourth line shows this router creating its open message to 172.16.1.2.

The fifth line shows this router sending its open message to 172.16.1.2 and changing its BGP state to open sent.

The sixth line shows this router receiving an acknowledgment for the open message that was sent to 172.16.1.2 and going to the open confirm state.

The seventh line indicates that the router is scanning (evaluating) the routing table for the pathways to send to the neighbor.

The last line shows that this router has agreed to form a BGP session with 172.16.1.2 by going to the established state.

BGP Idle and Established States

Cisco.com

- **Idle:** The router in this state cannot find the address of the neighbor in the routing table. Check for an IGP problem. Is the neighbor announcing the route?
- **Established:** The established state is the proper state for BGP operations. In the show ip bgp summary command, if the state column is blank or has a number, then the established state is in place. The number is how many routes have been learned from this neighbor.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-26

The idle state is an indication that the router does not know how to reach the IP address that is listed in the neighbor statement. The router is idle due to one of the following scenarios:

- It is waiting for a static route to that IP address or network.
- It is waiting for the local routing protocol (IGP) to learn about this network through an advertisement from another router.

The most common reason for the idle state is that the neighbor is not announcing the IP address or network that the neighbor statement of the router is pointing at. Check these two conditions first to correct this problem:

- Ensure that the neighbor announces the route in its local routing protocol (IGP).
- Verify that you have not entered an incorrect IP address in the neighbor statement.

The established state is the state that you want the neighbor relationship to be in. This state means that both routers have agreed to exchange BGP updates with one another and routing has begun.

BGP Active State Troubleshooting

Cisco.com

Active: The router has sent out an open packet and is waiting for a response. The state may cycle between active and idle. The neighbor may not know how to get back to this router because of the following reasons:

- Neighbor peering with the wrong address
- Neighbor does not have neighbor statement for this router
- Neighbor does not have a route to the source IP address of the BGP open packet generated by this router

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-27

If the router is in the active state, it means that it has found the IP address in the neighbor statement and has created and sent out a BGP open packet; however, the router has not received a response (open confirm packet) back.

One common problem in this case is that the neighbor may not have a return route to the source IP address.

Ensure that the source IP address or network of the packets has been announced to the local routing protocol (IGP).

Another common problem associated with the active state occurs when a BGP router attempts to peer with another BGP router that does not have a neighbor statement peering back at the first router, or the other router is peering with the wrong IP address on the first router.

Check to ensure that the other router has a neighbor statement peering at the correct address of the router that is in the active state.

If the state toggles between the idle state and the active state, one of the most common problems is AS number misconfiguration. You will see the following console message at the router with the wrong **remote-as** number configured in the neighbor statement:

```
6w0d: %BGP-3-NOTIFICATION: sent to neighbor 172.31.6.3 2/2  
(peer in wrong AS) 2 bytes FDE6
```

At the remote router, you will see the following message:

```
6w0d: %BGP-3-NOTIFICATION: received from neighbor 172.31.6.1  
2/2 (peer in wrong AS) 2 bytes FDE6
```

BGP Peering

Cisco.com

```
RouterA# show ip bgp summary
```

```
BGP table version is 23, main routing table version 23
10 network entries and 11 paths using 1242 bytes of memory
4 BGP path attribute entries using 380 bytes of memory
BGP activity 23/13 prefixes, 38/27 paths
0 prefixes revised.
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.100	4	65200	211	211	13	0	0	00:01:53	5
192.168.1.18	4	65101	214	226	23	0	0	00:00:13	1
192.168.1.34	4	65101	214	226	23	0	0	00:00:09	1
192.168.1.50	4	65101	214	225	23	0	0	00:00:06	3

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-28

The **show ip bgp summary** command is one way to verify the neighbor relationship. The figure presents a capture of the output from this command. The details of this command output are as follows:

- **BGP router ID:** IP address that all other BGP speakers recognize as representing this router.
- **BGP table version:** Increases in increments when the BGP table changes.
- **Neighbor:** The IP address that is used in the neighbor statement with which this router is setting up a relationship.
- **Version (V):** The version of BGP that this router is running with the listed neighbor.
- **AS:** The AS number of the listed neighbor.
- **Messages received (MsgRcvd):** The number of BGP messages that have been received from this neighbor.
- **Messages sent (MsgSent):** The number of BGP messages sent to this neighbor.
- **In queue (InQ):** The number of messages waiting to be processed from this neighbor.
- **Out queue (OutQ):** The number of messages queued up and waiting to be sent to this neighbor. TCP flow control prevents this router from overwhelming a neighbor with a large update.
- **Up/Down:** The length of time that this neighbor has been in the current BGP state (established, active, or idle).
- **State [established, active, idle, open sent, open confirm, or idle (admin)]:** The admin state is new to Cisco IOS software Release 12.0. Using a **neighbor** command under the **router bgp** command, you can set a neighbor to administratively shut down (admin state) with the following command:

```
neighbor ip-address-of-neighbor shutdown
```

- **Prefix received (PfxRcd):** When the session is in the established state, this number represents how many BGP network entries have been received from the listed neighbor.

BGP show, debug, and clear Commands

This topic presents common commands that are used in troubleshooting BGP and also presents various options for resetting the BGP session when changes are made to the neighbor relationships.

show ip bgp Command

Cisco.com

```
RouterA# show ip bgp

BGP table version is 23, local router ID is 192.168.1.49
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
*-> 10.0.0.0        10.1.1.100         0       0   65200  i
*-> 172.16.10.0/24  10.1.1.100         0       0   65200  i
*-> 172.16.11.0/24  10.1.1.100         0       0   65200  i
*>i172.26.1.16/28  192.168.1.50        0       100    0 i
*->i172.26.1.32/28 192.168.1.50        0       100    0 i
*->i172.26.1.48/28 192.168.1.50        0       100    0 i
*> 192.168.1.0     0.0.0.0           0       0   32768  i
*> 192.168.2.0     10.1.1.100         0       65200  65102  i
*> 192.168.2.64/28 10.1.1.100         0       65200  65102  i
* 1192.168.101.0   192.168.1.34        0       100    0 i
*>1                           192.168.1.18        0       100    0 i
```

The table displays networks from lowest network to highest.

Use the **show ip bgp** command to display the BGP topology database (BGP table).

In the figure, the first character to the left of the “Network” column should be an asterisk (*). This asterisk means that the next-hop address in the “Next Hop” column is reachable. The next-hop address is not always the router that is directly connected to this router.

The second character to the left of the “Network” column can be a greater than sign (>), which is the best path that is selected by BGP to forward to the IP routing table. The second character may also be an “s.” BGP uses “s” when you perform route summarization and suppress specific routes.

The second character can also be a “d” for dampening or an “h” for history. If a route has an “h” as the second character, that route is unavailable and is probably down. If the second character is a “d,” the route is being dampened (penalized) for going up and down too often. Although the route may be up right now, it is not advertised until the penalty has expired.

The third character to the left of the “Network” column is either blank or is an “i.” If it is blank, BGP learns that route from an external peer. If it is an “i”, an IBGP neighbor advertises this pathway to the router.

The “Next Hop” column lists all the next-hop addresses for each route. This column may also contain 0.0.0.0, which signifies that this router is the originator of the route for the network listed beside it.

The “Path” column signifies how this route was entered into BGP on the original router. If the last column has an “i” in it, the originating router probably used a network statement to introduce this network into BGP.

If the character is an “e,” this signifies that the originating router learned this network from EGP, which is the historical predecessor to BGP.

A question mark (?) signifies that BGP cannot absolutely verify the availability of this network because it is redistributed from an IGP into BGP.

The column with the “Path” header may contain a sequence of autonomous systems in the path. If you read the list of autonomous systems in this column from left to right, the first AS listed is the adjacent AS that this network was learned from.

The last number (rightmost AS number) is the originating AS of this network. The AS numbers between these two represent the exact pathway that a packet takes back to the originating AS. If the path column is blank, the route is from the current AS.

The three columns to the left of the “Path” column list three BGP path attributes that are associated with the path: metric (multi-exit discriminator, or MED), local preference, and weight.

Clearing the BGP Session

Cisco.com

- When policies such as access lists or attributes are changed, the BGP session must be reset.
- The change takes effect immediately, and the next time that a prefix or pathway is advertised or received, the new policy will be used. It can take a long time for the policy to be applied to all networks.
- The session should be reset to ensure that the policy is immediately applied to all affected prefixes and pathways.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-38

BGP can potentially handle huge volumes of routing information. When a policy configuration change occurs, the router cannot go through the huge table of BGP information and recalculate which entry is no longer valid in the local table. Nor can the router determine which route or routes, already advertised, should be withdrawn from a neighbor.

There is an obvious risk that the first configuration change will be immediately followed by a second, which would cause the whole process to start all over again. To avoid such a problem, Cisco IOS software applies changes only to those updates that are received or transmitted after the BGP policy configuration change has been performed. The new policy, enforced by the new filters, is applied only on routes that are received or sent after the change.

A network administrator who would like the policy change to be applied on all routes must force the router to let all routes pass through the new filter. If the filter is applied on outgoing information, the router has to resend the BGP table through the new filter. If the filter is applied on incoming information, the router needs its neighbor to resend its BGP table so that it passes through the new filters.

Traditionally, resetting the affected BGP sessions following a BGP policy configuration change has accomplished the goal of applying the policy change to all routes. After the BGP sessions are reset, all information received on those sessions is invalidated and removed from the BGP table. Also, the remote neighbor will detect a BGP session down state, and likewise will invalidate the routes that were received. After a period of 30 to 60 seconds, the BGP sessions are re-established automatically and the BGP table is exchanged again, but through the new filters. However, resetting the BGP session disrupts packet forwarding.

Resetting BGP Sessions

Cisco.com

router#

```
clear ip bgp *
```

- Resets all BGP connections with this router
- Entire BGP forwarding table is discarded
- BGP session makes the transition from established to idle; everything must be relearned

router#

```
clear ip bgp [ip-address]
```

- Resets only a single neighbor
- BGP session makes the transition from established to idle; everything from this neighbor must be relearned
- Better than clear ip bgp *

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-31

Resetting a session is a method of informing the neighbor or neighbors of a policy change. The two commands that are used for resetting both cause a hard reset of the BGP neighbors that are involved. A “hard reset” means that the router issuing either of these commands will close the appropriate TCP connections, re-establish those TCP sessions as appropriate, and resend all information to each of the neighbors affected by the particular command that is used.

By using **clear ip bgp ***, the BGP forwarding table on the router that issued this command is completely deleted and all networks must be relearned from every neighbor. If a router has multiple neighbors, this action is a very dramatic event. This command forces all neighbors to resend their entire tables simultaneously.

For example, consider a situation in which router A has eight neighbors and each neighbor has a full Internet table of about 32 MB in size. If router A issues the **clear ip bgp *** command, all eight routers will resend their 32-MB table at the same time. To hold all these updates, router A would need 256 MB of RAM. Router A would also need to be able to process all of this information. Processing 256 MB of updates would take a considerable amount of CPU cycles for router A, further delaying the routing of user data.

If the second command, **clear ip bgp [ip-address]**, is used, one neighbor is reset at a time. The impact is less severe on the router that is issuing this command; however, it takes longer to change policy for all of the neighbors, because each must be done individually as opposed to all at once using the **clear ip bgp *** command. The **clear ip bgp [ip-address]** command still performs a hard reset and must re-establish the TCP session with the specified address that is used in the command, but this command affects only a single neighbor at a time and not all neighbors at once.

The clear ip bgp soft out Option

Cisco.com

Router#

```
clear ip bgp {*|address} [soft out]
```

- Routes learned from this neighbor are not lost.
- This router resends all BGP information to the neighbor without resetting the connection.
- The connection remains established.
- This option is highly recommended when you are changing outbound policy.
- The soft out option does not help if you are changing inbound policy.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-32

The **soft** option of the **clear ip bgp** command allows BGP to do a soft reset for outbound updates. The router issuing the **soft out** command does not reset the BGP session; instead, the router creates a new update and sends the whole table to the specified neighbors.

This update includes withdrawal commands for those networks that you do not want the other neighbor to use anymore based on the new outbound policy.

The clear ip bgp soft in Option

Cisco.com

Router(config-router)#

```
neighbor [ip-address] soft-reconfiguration inbound
```

- A router BGP subcommand that notifies this router to store all updates from this neighbor in case the inbound policy is changed.
- The command is memory-intensive.

Router#

```
clear ip bgp {*|address} [soft in]
```

- Routes advertised to this neighbor are not withdrawn.
- This router stores all updates sent from this neighbor so new inbound policies can be evaluated without resetting the BGP session.
- The connection remains established.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-33

The **soft in** command can be memory-intensive. BGP does not allow a router to force another BGP speaker to resend its entire table. If you change the inbound BGP policy and you do not want to complete a hard reset, configure the router to perform a soft reconfiguration.

Enter the **neighbor** command that is shown in the figure to inform BGP to save all updates that were learned from the neighbor specified. The BGP router retains an unfiltered table of what that neighbor has sent. This unfiltered table is used when inbound policy is changed; the new results are placed in the BGP forwarding database. Thus, if you make changes, you do not have to force the other side to resend everything.

Note

Recent releases of Cisco IOS software contain a BGP Soft Reset Enhancement feature (route refresh), which provides automatic support for dynamic soft reset of inbound BGP routing table updates that is not dependent upon stored routing table update information. The new method requires no preconfiguration and requires significantly less memory than the previous soft reset method for inbound routing table updates. More information on this feature can be found on the Cisco website.

The show ip bgp neighbors Command

Cisco.com

```
RouterA# show ip bgp neighbors

BGP neighbor is 10.1.1.1, remote AS 65000, external link
Index 1, Offset 0, Mask 0x2
BGP version 4, remote router ID 172.16.10.1
BGP state = Established, table version = 5, up for 00:10:47
Last read 00:00:48, hold time is 180, keepalive interval is 60 seconds
Minimum time between advertisement runs is 30 seconds
Received 16 messages, 0 notifications, 0 in queue
Sent 15 messages, 1 notifications, 0 in queue
Prefix advertised 1, suppressed 0, withdrawn 0
Connections established 1; dropped 0
Last reset 00:16:35, due to Peer closed the session
2 accepted prefixes consume 64 bytes
0 history paths consume 0 bytes
--More--
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-34

Use the **show ip bgp neighbors** command to display information about the BGP connections to neighbors. In the figure, the BGP state is established, which means that the neighbors have established a TCP connection and the two peers have agreed to use BGP to communicate.

The debug ip bgp Command

Cisco.com

```
routerA# debug ip bgp updates

BGP updates debugging is on
RTRA# clear ip bgp *

3w5d: BGP: 10.1.1.1 computing updates, neighbor version 0, table
version 1, starting at 0.0.0.0
3w5d: BGP: 10.1.1.1 update run completed, ran for 0ms, neighbor
version 0, start version 1, throttled to 1, check point net 0.0.0.0
3w5d: BGP: 10.1.1.1 rcv UPDATE w/ attr: nexthop 10.1.1.1, origin i,
aggregated by 65000 172.16.10.1, path 65000
3w5d: BGP: 10.1.1.1 rcv UPDATE about 172.16.0.0/16
3w5d: BGP: nettable_walker 172.16.0.0/16 calling revise_route
3w5d: BGP: revise route installing 172.16.0.0/16 -> 10.1.1.1
3w5d: BGP: 10.1.1.1 rcv UPDATE w/ attr: nexthop 10.1.1.1, origin i,
metric 0, path 65000
3w5d: BGP: 10.1.1.1 rcv UPDATE about 192.168.1.0/24
3w5d: BGP: nettable_walker 192.168.1.0/24 calling revise_route
3w5d: BGP: revise route installing 192.168.1.0/24 -> 10.1.1.1
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-35

The figure highlights the received update messages that the router sends to its neighbor 10.1.1.1. The following output shows router A sending updates to its neighbor:

```
RTRA#
3w5d: BGP: 10.1.1.1 computing updates, neighbor version 0,
table version 1, starting at 0.0.0.0
```

Router A is reacting to the **clear ip bgp *** command of the administrator by recomputing and generating a new BGP routing update for neighbor 10.1.1.1. Router A will recompute starting with the lowest network number of 0.0.0.0 and continue until all networks have been examined.

The following output shows that router A has finished computing the routing update, which took less than 0 milliseconds:

```
3w5d: BGP: 10.1.1.1 update run completed, ran for 0ms,
neighbor version 0, start version 1, throttled to 1, check
point net 0.0.0.0
```

This output shows that router A has received an update from 10.1.1.1 with the next-hop, origin, and AS path attributes set for AS 65000, which was summarized by router ID 172.16.10.1 in AS 65000:

```
3w5d: BGP: 10.1.1.1 rcv UPDATE w/ attr: nexthop 10.1.1.1,
origin i, aggregated by 65000 172.16.10.1, path 65000
```

One of the networks in the update from 10.1.1.1 is 172.16.0.0 with a prefix mask of /16:

```
3w5d: BGP: 10.1.1.1 rcv UPDATE about 172.16.0.0/16
```

In order to install this network in the routing table for Router A, the next hop address must be reachable. So to reach network 172.16.0.0/16, Router A is examining the routing table to ensure that a valid pathway exists to the next-hop address:

```
3w5d: BGP: nettable_walker 172.16.0.0/16 calling revise_route
```

A valid pathway exists to the next hop address of 10.1.1.1, so the route to 172.16.0.0/16 is being installed in the routing table:

```
3w5d: BGP: revise route installing 172.16.0.0/16 -> 10.1.1.1
```

Note Debugging uses up router resources and should be turned on only when necessary.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **BGP is configured with the following basic BGP commands:**
 - router bgp *autonomous-system*
 - neighbor *ip-address* remote-as *autonomous-system*
 - network *network-number*
- **The show and debug commands are used to identify the states of a BGP peering relationship and to troubleshoot the BGP session.**
- **The clear ip bgp commands are used to reset BGP sessions.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-36

Next Steps

For the associated lab exercise, refer to the following sections of the course Lab Guide:

- Lab Exercise 7-1: Configuring EBGP for Two Neighbors
- Lab Exercise 7-2: Configuring Fully Meshed IBGP

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 command identifies to a BGP router if an IP address belongs to an IBGP or an EBGP neighbor?
- A) **neighbor {ip-address | peer-group-name} shutdown**
 - B) **neighbor {ip-address | peer-group-name} update-source interface-type interface-number**
 - C) **neighbor {ip-address | peer-group-name} remote-as autonomous-system**
 - D) **neighbor {ip-address | peer-group-name} next-hop-self**
- Q2) Which command sets the source IP address of a BGP update to be the IP address of a specific interface?
- A) **neighbor {ip-address | peer-group-name} shutdown**
 - B) **neighbor {ip-address | peer-group-name} update-source interface-type interface-number**
 - C) **neighbor {ip-address | peer-group-name} remote-as autonomous-system**
 - D) **neighbor {ip-address | peer-group-name} next-hop-self**
- Q3) Which one of the following BGP network statements is valid?
- A) network 199.199.199.199 mask 255.255.255.0
 - B) network 191.200.100.0
 - C) network 172.16.1.0 mask 255.255.0.0
 - D) network 200.100.50.0
- Q4) Which state indicates that the router does not have a pathway to the neighbor IP address?
- A) active
 - B) idle
 - C) established
 - D) open confirm
- Q5) Which state indicates that an open message has been sent but a reply has not been received from the neighbor in more than 5 seconds?
- A) active
 - B) idle
 - C) established
 - D) open confirm

- Q6) Which command is the most disruptive method of resetting BGP sessions and should be avoided?
- A) **clear ip bgp 192.168.200.1**
 - B) **clear ip bgp ***
 - C) **clear ip bgp 192.168.200.1 soft in**
 - D) **clear ip bgp 192.168.200.1 soft out**
- Q7) Which command resends the routing table without resetting the TCP session and flags all routes as either “withdrawals” or “inserts” to its neighbor, 192.168.200.1? (You should use this command if the outbound policy of a BGP router has changed.)
- A) **clear ip bgp 192.168.200.1**
 - B) **clear ip bgp ***
 - C) **clear ip bgp 192.168.200.1 soft in**
 - D) **clear ip bgp 192.168.200.1 soft out**

Quiz Answer Key

Q1) C

Relates to: Basic BGP Configuration

Q2) B

Relates to: Basic BGP Configuration

Q3) D

Relates to: Basic BGP Configuration

Q4) B

Relates to: BGP Neighbor States

Q5) A

Relates to: BGP Neighbor States

Q6) B

Relates to: BGP show, debug, and clear Commands

Q7) D

Relates to: BGP show, debug, and clear Commands

BGP Route Summarization

Overview

This lesson explains how Border Gateway Protocol version 4 (BGP4) performs classless interdomain routing (CIDR) and demonstrates two methods for performing summarization for BGP.

Relevance

Route summarization for BGP is required for the Internet. A BGP administrator must know the various methods to accomplish this route summarization.

Objectives

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

- Explain how BGP4 is related to CIDR
- Explain how BGP implements route summarization with the **network** command
- Describe how BGP implements route summarization with the **aggregate-address** command

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience
- Knowledge of IP subnetting, including complex subnetting and variable-length subnet masking (VLSM)

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **BGP Version 4 and Classless Interdomain Routing**
- **BGP Route Summarization Using the network Command**
- **BGP Route Summarization Using the aggregate-address Command**
- **Summary**
- **Quiz**

BGP Version 4 and Classless Interdomain Routing

This topic explains the relationship between BGP4 and CIDR. In addition, the circumstances under which BGP4 specifies networks, and the methods that are used by BGP4 in this process, are discussed.

CIDR and Aggregate Addresses

Cisco.com

- With BGP4, routes can be aggregated by any AS on any BGP router.
- BGP4 is classless, supports VLSM and longest match routing, and carries a network mask for each network in the update.

```
graph TD; B((B AS 65000)) --> A((A AS 64520)); C((C AS 65250)) --> A; D((D AS 65500)) --> A; A -- "192.168.0.0/16" --> B;
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-4

CIDR is a mechanism that was developed to address the problem of the exhaustion of IP addresses and the growth of routing tables. For CIDR, blocks of multiple class C addresses are combined or aggregated to create a larger classless set of IP addresses. These multiple class C addresses are then summarized in routing tables, resulting in fewer route advertisements.

Earlier versions of BGP did not support CIDR. BGP4 support for CIDR includes the following features:

- The BGP update message includes both the prefix and prefix length. Previous versions included only the prefix, and the address class specified the length.
- Addresses can be aggregated when they are advertised by a BGP router.
- The AS path attribute includes a combined list of all autonomous systems that the aggregated routes have passed through. This combined list is used to ensure that the route is loop-free.

In the figure, router C advertises network 192.168.2.0/24, and router D advertises network 192.168.1.0/24. Router A passes those advertisements to router B; however, router A reduces the size of the routing tables by aggregating the two routes into one, such as 192.168.0.0/16.

Two BGP attributes related to aggregate addressing are the following:

- **Atomic aggregate:** A discretionary attribute that informs the neighbor AS that the originating router has aggregated the routes.
- **Aggregator:** An optional transitive attribute that specifies the BGP router ID and AS number of the router that performed the route aggregation.

By default, the aggregate route is advertised as coming from the AS that performs the aggregation. This route has the atomic aggregate attribute set to show potential missing information.

The AS numbers in the nonaggregated routes are not listed. The aggregation router can be configured to include the list of all autonomous systems that are contained in all paths that are being summarized.

In the figure, the aggregated route 192.168.0.0/16 has an AS path attribute of (64520) by default. If router A is configured to include the combined list, then it includes the set of (65250, 65500) as well as (64520) in the AS path attribute.

Note	In the figure, the aggregate route that is sent by router A covers more routes than the two from routers C and D. The example assumes that router A has jurisdiction over all the other routes covered by this aggregate route.
-------------	---

Network Boundary Summarization

Cisco.com

```
Router(config-router)#  
no auto-summary
```

- **BGP, RIPv1 and RIPv2, IGRP, and EIGRP perform network boundary summarization by default.**
- **BGP, RIPv2, and EIGRP can disable network boundary summarization.**
- **CIDR has forced the IANA to begin using class A addresses, like 64.0.0.0, in a classless manner.**
- **If you are assigned a portion of a class A, B, or C address, the no-auto summary command needs to be implemented under the BGP process or you risk claiming ownership of the whole class A, B, or C address.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 7-5

Routing Information Protocol version 1 (RIPv1), Routing Information Protocol version 2 (RIPv2), IGRP, and EIGRP perform network boundary summarization by default. In contrast, OSPF and IS-IS perform all summarization manually.

BGP also performs classful summarization by default. This feature may need to be turned off. The IANA is reclaiming class A addresses from organizations that no longer need them. IANA breaks these class A addresses into blocks of /19 address space. The blocks of addresses are assigned to various ISPs to be given out in place of class C addresses. This process has helped make the Internet a classless environment.

The BGP **auto-summary** command is also responsible for the behavior of the redistribution procedure in BGP. When enabled, all redistributed subnets are summarized to their classful boundaries in the BGP table. When disabled, all redistributed subnets are present in their original form in the BGP table.

For example, if an ISP assigns a network of 64.100.50.0/24 to an AS, and that AS then uses the **redistribute connected** command to introduce this network into BGP, BGP announces that the AS owns 64.0.0.0/8 if the **auto-summary** command is left on. To the Internet, this AS owns all of the class A network 64.0.0.0/8, which is not true. Other organizations that own a portion of the 64.0.0.0/8 address space may have connectivity problems because this AS has claimed ownership for the whole block of addresses. This outcome is not desirable if the AS does not own the entire address space.

Using the **network 64.100.50.0 mask 255.255.255.0** command instead of the **redistributed connected** command will ensure that this assigned network is correctly announced.

Example

BGP was originally not intended to advertise subnets. Its intended purpose was to advertise classful networks or better. By “better,” it is meant that BGP can summarize blocks of individual classful networks into a few large blocks that represent the same amount of address space as the individual network block.

This process is called CIDR. For example, 32 contiguous class C networks can be advertised individually as 32 separate entries with each having a network mask of /24, or it may be possible to announce these same networks as a single entry with a /19 mask.

By default, when BGP recognizes at least one subnet of a classful address space and has a network statement for the classful address, it announces the classful network and not the subnet.

For example, if a BGP router has network 170.16.22.0/24 in the routing table as a directly connected network, and a network statement of network 172.16.0.0 under BGP, BGP announces the 172.16.0.0/16 network to all neighbors. If 172.16.22.0 was the only subnet for this network in the routing table and it became unavailable,

BGP would withdraw the 172.16.0.0/16 from all neighbors. If the network statement of network 172.16.22.0 mask 255.255.255.0 was used instead of network 172.16.0.0, BGP would announce 172.16.22.0/24 and not 172.16.0.0/16.

BGP Route Summarization Using the network Command

This topic demonstrates how to perform BGP summarization using the **network** command and a static route pointing at the null0 interface.

BGP network Command

Cisco.com

```
Router(config-router)#  
    network network-number [mask network-mask]
```

- This command was not designed to perform summarization by itself. The aggregate-address command was designed for summarization.

```
Router(config)#  
    ip route prefix mask null0
```

- To use the network statement for summarization, the network number and mask used must already exist in the routing table.
- If the route was already summarized by EIGRP or OSPF, that summarization can be announced into BGP with the network and mask commands.
- If the route was not already summarized, a null route must be created for BGP to announce this summarization.

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 7-6

The **network** command with the **mask** option installs a prefix into the BGP table when a matching IGP prefix exists in the IP routing table. If the IGP prefix flaps (route removed from routing table), the BGP prefix also flaps.

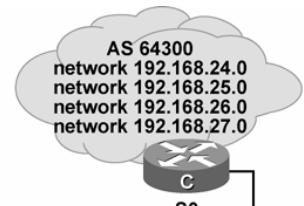
Several ways to advertise the prefix in BGP exist. In the case of a simple classful network number, use the **network prefix** command without the **mask** option. If you are aggregating prefixes that originate in this AS, use the **network prefix mask mask** command.

Note	The network command requires that there be an exact match for the prefix or mask that is specified in the forwarding table. This exact match can be accomplished by using a static route with a null0 interface, or it can already exist in the routing table because the IGP has performed the summarization.
-------------	---

Cautions about Network Statement

Cisco.com

- If a network statement is used for summarization, do not use the more specific entries and the summarized route as shown here.
- If both are used, the summarized route and the more specific routes will be announced.
- 192.168.24.0/22 does not exist in the IP routing table without the null route. BGP will not announce the network unless the summarized route is already present in the routing table.



```
router bgp 64300
network 192.168.24.0
network 192.168.25.0
network 192.168.26.0
network 192.168.27.0
network 192.168.24.0 mask 255.255.252.0
neighbor 172.16.2.1 remote-as 64200
ip route 192.168.24.0 255.255.252.0 null 0
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-7

The **network** command under the **router bgp** command informs BGP what to advertise, but not how to advertise those networks. When you are using the network statement under **router bgp**, before BGP can announce any specified network, the network number that is specified must also be in the IP routing table. For example, consider the group of addresses 192.168.24.0/24, 192.168.25.0/24, 192.168.26.0/24, and 192.168.27.0/24 that are already in the routing table.

You can put the following network statements under **router bgp**:

```
router bgp 64300
network 192.168.24.0
network 192.168.25.0
network 192.168.26.0
network 192.168.27.0
```

Each of the class C networks here is announced because they already exist in the routing table. You can summarize these networks with the following command:

```
router bgp 64300
network 192.168.24.0 mask 255.255.252.0
```

The 192.168.24.0/22 address is not announced because that route is not in the routing table. If the local routing protocol supports summarization (such as EIGRP or OSPF), and summarization is performed using the local interior routing protocol command, BGP will announce that route.

If route summarization is not performed with the local interior routing protocol and BGP is required to announce this route, a static route should be created that allows this network to be

installed in the routing table. The static route should be pointed at the null 0 interface (ip route 192.168.24.0 255.255.252.0 null 0).

Remember that the 192.168.24.0/24, 192.168.25.0/24, 192.168.26.0/24, and 192.168.27.0/24 addresses are already in the routing table. This command creates an additional entry of 192.168.24.0/22 as a static route to null 0. Use the longest match for routing decisions so that the null 0 route is not used unless one of the more specific networks is unreachable.

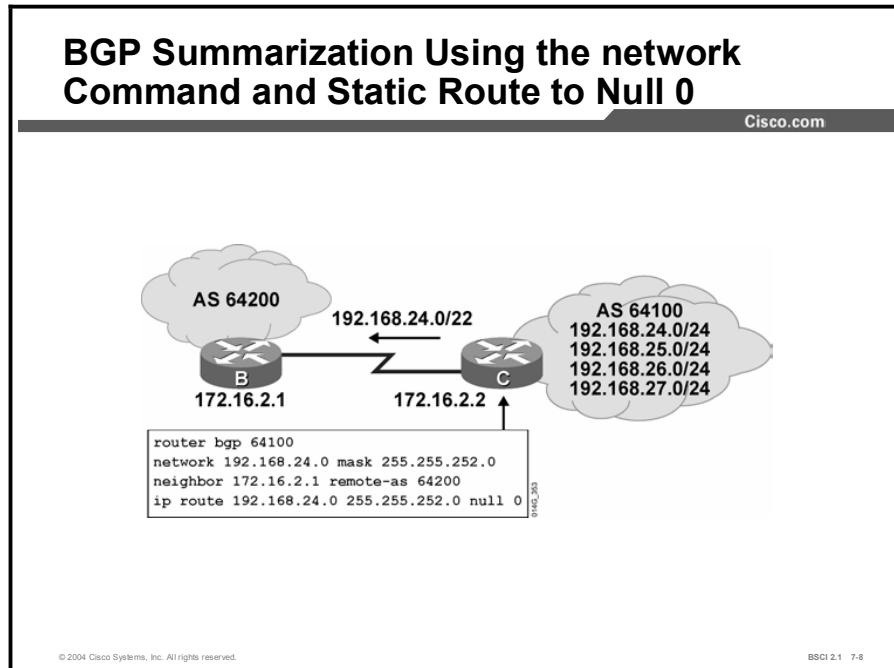
If a network, such as 192.168.25.0/24, is unreachable and packets arrive from the ISP to AS 64300 going to 192.168.25.1, the destination address is compared to the current entries in the routing table using the longest-match criteria. Because 192.168.25.0/24 does not exist in the routing table, the best match is 192.168.24.0/22, which is pointing at the null 0 interface.

The packets are sent to the null 0 interface and an Internet Control Message Protocol (ICMP) unreachable message is generated and sent to the originator of the packets. Dropping these packets prevents traffic from using up bandwidth by following a default route that is either deeper into your AS or (in a worst-case scenario) back out to the ISP. The ISP would then route the packets back to the AS because of the summarized route that was advertised to the ISP, causing a routing loop.

In the figure, all five networks are announced using network statements for the more specific routes and for the summarized route. The purpose of summarization is to reduce the size of the advertisement, as well as the size of the Internet routing table.

Announcing these more specific networks along with the summarized route actually increases the size of the table. The table increases in size because five routes are announced instead of four (with no summarization) or one (with proper summarization).

Example



In the figure, the configuration for AS 64100 is more efficient because there is a single entry to represent all four networks and a **static null route** command to install the summarized route in the IP routing table so that BGP can find a match.

The AS 64100 router advertises a summarized route for the four class C addresses (192.168.24.0/24, 192.168.25.0/24, 192.168.26.0/24, and 192.168.27.0/24) that are assigned to the AS with the network statement. For the new network statement (192.168.24.0/22) to be advertised, it must first appear in the local routing table.

Because only the more specific networks exist in the IP routing table, a static route pointing to null 0 has been created to allow BGP to announce this network (192.168.24.0/22) to AS 64200.

BGP Route Summarization Using the aggregate-address Command

This topic shows how to use the **aggregate-address** command to perform route summarization for BGP.

Configuring BGP for Aggregate Addressing

Cisco.com

```
Router(config-router)#  
aggregate-address ip-address mask [summary-only]  
[as-set]
```

- Creates an aggregate (summary) entry in the BGP table
- Uses the summary-only option to advertise only the summary and not the specific routes
- Adds the as-set option to include a list of all the autonomous system numbers that the more specific routes have passed through
- Recommended method of summarization for BGP
- Null static route not needed; BGP null route automatically generated

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 7-9

Use the **aggregate-address** command to create an aggregate, or summary, entry in the BGP table. The following table describes the command parameters.

Table 1: The aggregate-address Command Parameters

Parameter	Description
ip-address	The aggregate address to be created.
mask	The mask of the aggregate address to be created.
summary-only	(Optional) Causes the router to advertise only the aggregated route. The default is to advertise both the aggregate and the more specific routes.
as-set	(Optional) Generates AS path information with the aggregate route to include all the AS numbers that are listed in all the paths of the more specific routes. The default for the aggregate route is to list only the AS number of the router that generated the aggregate route.

With this command, the aggregate route is advertised as coming from the AS and has the atomic aggregate attribute set to show if any information is missing.

Note By default, the atomic aggregate attribute is set unless the **as-set** keyword is specified.

The **aggregate-address** *address mask* [**summary-only**] command advertises the summary network only, and suppresses the detailed routes.

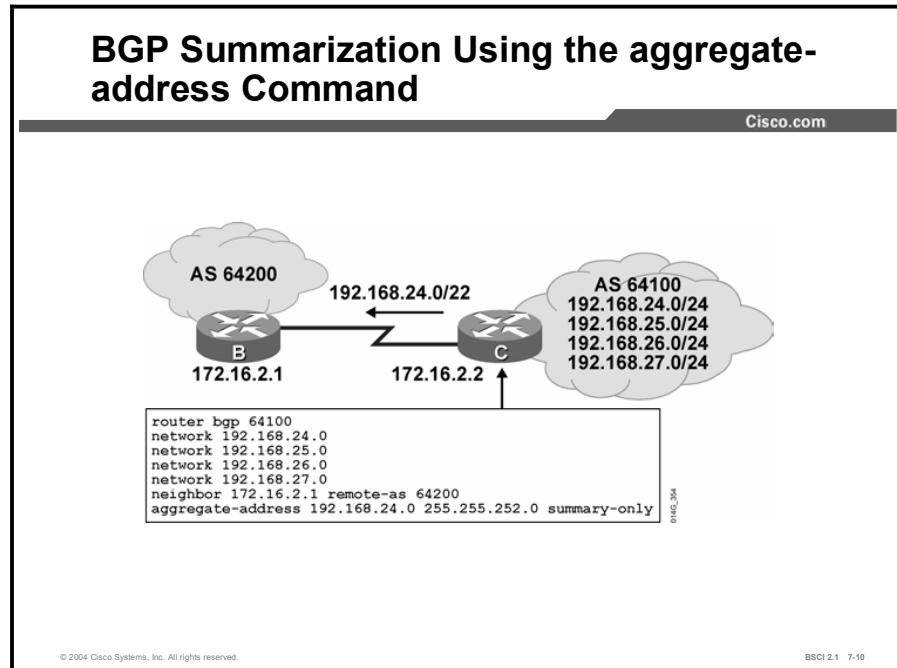
When you use the **aggregate-address** command, a null BGP route is automatically installed in the IP routing table for this summarized route.

If any route already in the BGP table is within the range indicated by the **aggregate-address** command, then the summary route is inserted into the BGP table and advertised to other routers.

This process creates more information in the BGP table. To get any benefits from the aggregation, the more specific routes, which are covered by the route summary, should be suppressed. This condition is achieved by the **summary-only** option.

When the more specific routes are suppressed, they are still present in the BGP table of the router doing the aggregation. However, because the routes are marked as suppressed, they are never advertised to any other router.

Example



This figure shows the following:

- **router bgp 64100:** Configures a BGP process for AS number 64100
- **network statements:** Configure BGP to advertise the following class C networks.
network 192.168.24.0
network 192.168.25.0
network 192.168.26.0
network 192.168.27.0
- **neighbor 172.16.2.1 remote-as 64200:** Specifies the router at this address as a neighbor in AS 64200. This part of the example describes whom to send the advertisements to.
- **aggregate-address 192.168.24.0 255.255.252.0 summary-only:** Specifies the aggregate route to be created, but suppresses advertisements of more specific routes to all neighbors. This part of the example describes how to advertise. Without the **summary-only** option, the new summarized route is advertised along with the more specific routes.

The following condition must be met for BGP to announce a summary route using the **aggregate-address** command: BGP must recognize the network to be advertised; at least one of the more specific routes must be in the BGP table.

BGP recognizes the routes because the network statements for those routes are present. The **aggregate-address** command tells BGP to perform route summarization and automatically installs the null route representing the new summarized route.

The AS 64200 router receives only one network (192.168.24.0/22) from AS 64100. Only one network is received because of the **summary-only** option on the **aggregate-address** command on router C in AS 64100.

The **network** command tells BGP what to advertise.

The **aggregate-address** command tells BGP how to advertise the networks.

The **aggregate-address** command does not replace a **network** command; at least one of the more specific routes must be in the BGP table.

In some situations, the more specific routes are injected into the BGP table by some routers and the aggregation is done in another router or even in another AS. This approach is called “proxy aggregation.” In this case, the aggregation router will need only the proper **aggregate-address** command, and not the **network** commands, to advertise the more specific routes.

BGP Aggregation

Cisco.com

RouterC#

```
show ip bgp
```

```
routerC# show ip bgp
```

```
BGP table version is 28, local router ID is 172.16.2.1
status codes: s = suppressed, * = valid, > = best, and i = internal
origin codes : i = IGP, e = EGP, and ? = incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.168.24.0/22	0.0.0.0	0		32768	i
s> 192.168.24.0	0.0.0.0	0		32768	i
s> 192.168.25.0	0.0.0.0	0		32768	i
s> 192.168.26.0	0.0.0.0	0		32768	i
s> 192.168.27.0	0.0.0.0	0		32768	i

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-11

The **show ip bgp** command displays the local router ID, the networks that are recognized by BGP, the accessibility to remote networks, and AS path information. In the figure, notice the “s” in the first column for the bottom four networks.

These networks are being suppressed. They were learned from a network statement on this router because the next-hop address is 0.0.0.0, which indicates that this router created these entries in BGP.

Notice that this router created the summarized route 192.168.24.0/22 in BGP, and that this network has a next hop of 0.0.0.0, indicating that the router created it. The more specific routes are suppressed and only the summarized route is announced.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **BGP4 supports CIDR with update messages including the prefix and length, aggregate addresses advertised by a router, and a combined list of all the autonomous systems that the aggregated routes have passed through.**
- **The network command with the mask option or the aggregate-address command can be used to perform BGP route summarization.**
- **The network command requires the exact match of the prefix and mask in the IP routing table. It might require a static route to the null 0 interface.**
- **The aggregate-address command requires a more specific prefix in the BGP table.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-12

References

For additional information, refer to these resources:

- RFC 1518, *An Architecture for IP Address Allocation with CIDR*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 2050, *Internet Registry IP Allocation Guidelines*

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) Consider the following configuration and routing table for router A (assume default settings for everything else):

```
router bgp 65001
neighbor 192.168.1.1 remote-as 65002
network 172.16.0.0
network 10.1.0.0 mask 255.255.0.0
show ip route
10.0.0.0 /8 is variably subnetted. 3 subnets
C      10.2.1.0/24 is directly connected, Ethernet 0/0
O      10.2.2.0/24 [110/870] via 10.2.1.1, 00:00:03, Ethernet
0/0
O      IA      10.1.0.0/16 [110/990] via 10.2.1.1, 00:00:03,
Ethernet 0/0
172.16.0.0/24 is subnetted, 2 subnets
O      172.16.1.0/24 [110/660] via 10.2.1.1, 00:00:03, Ethernet
0/0
O      172.16.2.0 /24 [110/770] via 10.2.1.1, 00:00:03,
Ethernet 0/0
```

What networks are announced by BGP?

- A) Router A announces 172.16.1.0/24 and 10.1.0.0/16.
 - B) Router A announces 10.0.0.0/8.
 - C) Router A announces 172.16.0.0/16 and 10.1.0.0/16.
 - D) Router A announces 172.16.0.0 /16.
- Q2) Which three characteristics describe the default behavior of BGP4? (Choose three.)
- A) supports VLSM
 - B) performs no summarization
 - C) supports classless routing
 - D) uses the longest-match criteria to select the appropriate route

Q3) Examine this configuration:

```
router bgp 65000
neighbor 172.16.1.1 remote-as 64400
network 192.168.8.0 mask 255.255.248.0
```

Which two requirements should be satisfied for the 192.168.8.0/21 CIDR block to be announced to neighbor 172.16.1.1? (Choose two.)

- A) A static route pointing to null 0 for network 192.168.8.0/21 must be configured on this router.
- B) The eight class C addresses (192.168.8.0 to 192.168.15.0) with a /24 mask that make up this CIDR block must be reachable by AS 65000.
- C) If this router is running EIGRP for its IGP, another EIGRP router must advertise a summarized route for 192.168.8.0/21.
- D) The autosummary must be turned off for this **network** command to work.

Q4) Which command announces only the summarized block of 192.168.0.0/16, suppresses the more specific networks, and installs a BGP route to null 0 for this summarization in the routing table?

- A) **aggregate-address 192.168.0.0 255.255.0.0**
- B) **network 192.168.0.0 mask 255.255.0.0**
- C) **aggregate-address 192.168.0.0 255.255.0.0 summary-only**
- D) **aggregate-address 192.168.0.0 255.255.0.0 as-set**

Q5) In the **show ip bgp** command, what does the “s” in front of a network mean?

- A) summarized network
- B) subnet of a network
- C) suppressed network
- D) supernet of a network

Quiz Answer Key

Q1) C

Relates to: BGP Version 4 and Classless Interdomain Routing

Q2) A, C, D

Relates to: BGP Version 4 and Classless Interdomain Routing

Q3) A, C

Relates to: BGP Route Summarization Using the network Command

Q4) C

Relates to: BGP Route Summarization Using the aggregate-address Command

Q5) C

Relates to: BGP Route Summarization Using the aggregate-address Command

BGP Path Selection Process

Overview

This lesson explains the various BGP attributes, the characteristics of each, and how they are evaluated for BGP to select the best pathway to a given network.

Relevance

BGP is used to perform policy-based routing (PBR). In order to manipulate the best pathways chosen by BGP, a network administrator must understand the different attributes that BGP uses and how BGP selects the best pathway based on these attributes.

Objectives

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

- List the characteristics of BGP attributes
- Describe the AS path attribute
- Identify the characteristics of the next-hop attribute and its behavior
- Describe the origin attribute
- Describe the local preference attribute and its usage
- Describe the MED attribute and its usage
- Describe the weight attribute and its usage
- Describe BGP path selection criteria
- Explain the BGP path selection decision process

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience
- Routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Characteristics of BGP Attributes**
- **The AS Path Attribute**
- **The Next-Hop Attribute**
- **The Origin Attribute**
- **The Local Preference Attribute**
- **The MED Attribute**
- **The Weight Attribute**
- **BGP Path Selection Criteria**
- **The BGP Path Selection Decision Tree**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-3

Characteristics of BGP Attributes

This topic identifies the attributes that BGP uses to describe the pathways to each network. Each attribute has characteristics that inform BGP routers receiving updates about how to treat the attribute.

BGP Path Attributes

Cisco.com

- **BGP metrics are called path attributes.**
- **Characteristics of path attributes include:**
 - **Well-known versus optional**
 - **Mandatory versus discretionary**
 - **Transitive versus nontransitive**
 - **Partial**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-4

BGP routers send BGP update messages about destination networks to other BGP routers. The BGP update messages contain one or more routes and a set of attributes attached to the routes.

The characteristics of an attribute are well-known or optional; mandatory or discretionary; transitive or nontransitive; and may also be partial.

Not all combinations of these characteristics are valid. Path attributes fall into the following four separate categories:

- Well-known mandatory
- Well-known discretionary
- Optional transitive
- Optional nontransitive

Only optional transitive attributes can be marked as partial.

Well-Known Attributes

Cisco.com

- **Well-known attributes**
 - Must be recognized by all compliant BGP implementations
 - Are propagated to other neighbors
- **Well-known mandatory attributes**
 - Must be present in all update messages
- **Well-known discretionary attributes**
 - May be present in update messages

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

All BGP routers must recognize a well-known attribute and propagate it to the other BGP neighbors.

Well-known attributes are either mandatory or discretionary. A well-known mandatory attribute must be present in all BGP updates. However, a well-known discretionary attribute does not have to be present in all BGP updates.

Optional Attributes

Cisco.com

- **Optional attributes**
 - Recognized by some implementations (could be private); expected not to be recognized by everyone
 - Recognized optional attributes are propagated to other neighbors based on their meaning
- **Optional transitive attributes**
 - If not recognized, are marked as partial and propagated to other neighbors
- **Optional nontransitive attributes**
 - Discarded if not recognized

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-6

Attributes that are not well-known are called optional. All BGP routers do not need to support an optional attribute. Optional attributes are either transitive or nontransitive.

The following statements apply to optional attributes:

- BGP routers that implement the optional attribute may propagate it to the other BGP neighbors.
- BGP routers that do not implement an optional transitive attribute should pass it to other BGP routers untouched and mark the attribute as partial.
- BGP routers that do not implement an optional nontransitive attribute must delete the attribute and not pass it to other BGP routers.

BGP Attributes

Cisco.com

BGP attributes include the following:

- **AS path ***
- **Next-hop ***
- **Local preference**
- **Multi-exit discriminator (MED)**
- **Origin ***
- **Others**

* Well-known mandatory attribute

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-7

The following is a list of the common BGP attributes according to the different categories that they belong to:

- Well-known mandatory attributes:
 - AS path
 - Next-hop
 - Origin
- Well-known discretionary attributes:
 - Local preference
 - Atomic aggregate
- Optional transitive attribute:
 - Aggregator
- Optional nontransitive attribute:
 - Multi-exit discriminator (MED)

Note In addition, Cisco uses a weight attribute for BGP. The weight attribute is an attribute that is defined by Cisco. The weight is configured locally on a router and is not propagated to any other BGP routers.

The AS Path Attribute

This topic defines the well-known, mandatory, transitive attribute known as AS path.

AS Path Attribute

Cisco.com

- **A list of autonomous systems that a route has traversed**
 - For example, on router B, the path to 192.168.1.0 is the AS sequence (65500, 64520).
- **The AS path attribute is well-known, mandatory, and transitive.**

0145-365

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-8

Whenever a route update passes through an AS, the AS number is prepended (added) to that update when it is advertised to the next EBGP neighbor. The AS path attribute is actually the list of AS numbers that a route has traversed to reach a destination.

Example

In the figure, router A in AS 64520 advertises network 192.168.1.0. When that route traverses AS 65500, router C prepends its own AS number to it. When 192.168.1.0 reaches router B, it has two AS numbers attached to it. From the perspective of router B, the path to reach 192.168.1.0 is (65500, 64520).

A similar process applies for the paths to networks 192.168.2.0 and 192.168.3.0. The path from router A to 192.168.2.0 is (65500, 65000), which means traverse AS 65500 and then AS 65000. Router C will have to traverse path (65000) to reach 192.168.2.0, and path (64520) to reach 192.168.1.0.

The Next-Hop Attribute

This topic defines the well-known, mandatory, transitive attribute known as the next-hop attribute.

Next-Hop Attribute

Cisco.com

The IP address of the next AS to reach a given network:

- Router A advertises network 172.16.0.0 to router B in EBGP, with a next hop of 10.10.10.3.
- Router B advertises 172.16.0.0 in IBGP to router C, keeping 10.10.10.3 as the next-hop address.

The next-hop attribute is well-known, mandatory, and transitive.

AS 65000

172.20.0.0 172.20.10.1 172.20.10.2

B C

10.10.10.1

10.10.10.3

A

172.16.0.0 AS 64520

014C_368

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 7-9

The BGP next-hop attribute is a well-known mandatory attribute that indicates the next-hop IP address that is to be used to reach a destination. BGP routes AS by AS, not router by router. The next-hop address of a network from another AS will be an IP address of the entry point of the next AS along the pathway to that destination network.

Example

For EBGP, the next hop is the IP address of the neighbor that sent the update. In the figure, router A will advertise 172.16.0.0 to router B, with a next hop of 10.10.10.3, and router B will advertise 172.20.0.0 to router A, with a next hop of 10.10.10.1.

For IBGP, the protocol states that the next hop that is advertised by EBGP should be carried into IBGP. Because of that rule, router B will advertise 172.16.0.0 to its IBGP peer router C with a next hop of 10.10.10.3 (router A address). Therefore, router C knows that the next hop to reach 172.16.0.0 is 10.10.10.3, not 172.20.10.1.

It is very important for router C to know how to reach the 10.10.10.0 subnet, either via an IGP or a static route; otherwise, it will drop packets destined to 172.16.0.0 because it will not be able to get to the next-hop address for that network.

The Origin Attribute

This topic defines the well-known, mandatory, transitive attribute known as origin.

Origin Attribute

Cisco.com

- **IGP (i)**
 - network **command**
- **EGP (e)**
 - **Redistributed from EGP**
- **Incomplete (?)**
 - **Redistributed from IGP or static**

The origin attribute informs all Autonomous Systems in the internetwork how the prefixes were introduced into BGP.

The origin attribute is well-known, mandatory, and transitive.

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 7-10

The origin attribute defines the origin of the path information. The origin attribute can be one of the following three values:

- **IGP:** The route is interior to the originating AS. This value normally happens when the **network** command is used to advertise the route via BGP. An origin of IGP is indicated with an “i” in the BGP table.
- **EGP:** The route has been learned via the EGP. This value is indicated with an “e” in the BGP table. EGP is considered a historical routing protocol and is not supported on the Internet because it performs only classful routing and does not support CIDR.
- **Incomplete:** The origin of the route is unknown or has been learned via some other means. This value usually occurs when a route is redistributed into BGP. An incomplete origin is indicated with a “?” in the BGP table.

The Local Preference Attribute

This topic defines the well-known, discretionary, nontransitive attribute known as local preference.

Local Preference Attribute

Paths with highest preference value are most desirable:

- Local preference is used to advertise to IBGP neighbors about how to leave their AS.
- The local preference is sent to IBGP neighbors only.

The local preference attribute is well-known and discretionary, and is passed only within the AS.

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 7-11 0140_357

Local preference is a well-known discretionary attribute that provides an indication to routers in the AS about which path is preferred to exit the AS. A path with a higher local preference is preferred.

The local preference is an attribute that is configured on a router and exchanged among routers within the same AS only. The default value for local preference on a Cisco router is 100.

Example

In the figure, AS 64520 receives updates about network 172.16.0.0 from two directions. The local preference on router A is set to 200, and the local preference on router B is set to 150.

Because the local preference information is exchanged within AS 64520, all traffic in AS 64520 addressed to network 172.16.0.0 will be sent to router A as an exit point from AS 64520 because of the higher local preference.

The MED Attribute

This topic defines the MED attribute.

MED Attribute

Cisco.com

The paths with the lowest MED (also called the metric) value are the most desirable:

- MED is used to advertise to EBGP neighbors how to exit their AS to reach networks owned by this AS.
- MED is sent to EBGP neighbors only.

The MED attribute is optional and nontransitive.

0140_368

© 2004 Cisco Systems, Inc. All rights reserved.BSCI 2.1 7-12

The MED attribute, also called the metric, is an optional nontransitive attribute.

The MED is an indication to EBGP neighbors about the preferred path into an AS. The MED attribute is a dynamic way to influence another AS about which path that it should choose to reach a certain route when multiple entry points into an AS exist. A lower metric is preferred.

Unlike local preference, the MED is exchanged between autonomous systems. The MED is carried into an AS and used there, but it is not passed on to the next AS. When the same update is passed on to another AS, the metric will be set back to the default of 0. MED influences inbound traffic to an AS, and local preference influences outbound traffic from an AS.

By default, a router will compare the MED attribute only for paths from neighbors in the same AS.

Note By using the MED attribute, BGP is the only protocol that can affect how routes are sent into an AS.

Example

In the figure, the router B MED attribute is set to 150, and the router C MED attribute is set to 200. When router A receives updates from routers B and C, it picks router B as the best next hop because a MED of 150 is less than 200.

The Weight Attribute

This topic defines the Cisco proprietary weight attribute.

Weight Attribute (Cisco Only)

The diagram illustrates a network topology with four routers (B, D, C, A) and three Autonomous Systems (AS 65000, AS 65250, AS 65500). Router A is located in AS 64520 and has two paths to 172.20.0.0: one from router B (Weight = 200) and one from router C (Weight = 150). Router A's path to router B is highlighted with a thicker arrow. Router A also has a direct connection to router D.

Paths with the highest weight value are most desirable.

- Weight not sent to any BGP neighbors

© 2004 Cisco Systems, Inc. All rights reserved. BSCI 2.1 7-13

The weight attribute is an attribute that Cisco defines for the path selection process. The weight is configured locally on a router and is not propagated to any other routers. This attribute applies when you are using one router with multiple exit points out of an AS, as opposed to the local preference attribute that is used when two or more routers provide multiple exit points.

The weight can have a value from 0 to 65535. Paths that the router originates have a weight of 32768 by default, and other paths have a weight of 0 by default.

Routes with a higher weight are preferred when multiple routes exist to the same destination.

Example

In the figure, routers B and C learn about network 172.20.0.0 from AS 65250 and propagate the update to router A. Router A has two ways to reach 172.20.0.0, and it has to decide which route to take.

In the example, router A sets the weight of updates coming from router B to 200 and the weight of those coming from router C to 150. Because the weight for router B is higher than the weight for router C, router A uses router B as a next hop to reach 172.20.0.0.

BGP Path Selection Criteria

This topic discusses how BGP chooses a route for submission to the IP routing table.

BGP Route Selection

Cisco.com

- **The BGP forwarding table usually has multiple pathways from which to choose for each network.**
- **BGP is not designed to perform load balancing:**
 - Paths are chosen because of policy.
 - Paths are not chosen based upon bandwidth.
- **The BGP selection process eliminates any multiple pathways through attrition until a single best pathway is left.**
- **That best pathway is submitted to the routing table manager process and evaluated against the methods of other routing protocols for reaching that network (administrative distance).**
- **The routing protocol with the lowest administrative distance will be installed in the routing table.**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-14

Multiple pathways may exist to reach a given network. As pathways for the network are evaluated and determined not to be the best path, they are eliminated from the selection criteria but kept in the BGP forwarding table (which can be displayed using the **show ip bgp** command) in case the best path becomes inaccessible.

For example, suppose there are seven pathways to reach network 10.0.0.0. All pathways have no AS loops and have valid next-hop addresses, so all seven paths proceed to step 1, which examines the weight of the paths.

All seven paths have a weight of 0, so they all proceed to step 2, which examines the local preference of the paths. Four of the paths have a local preference of 200 and the other three have local preferences of 100, 100, and 150.

The four with a local preference of 200 will continue the evaluation process to the next step. The other three will still be in the BGP forwarding table, but are currently disqualified as the best path.

BGP will continue the evaluation process until only a single best pathway remains. The single best pathway that remains will be submitted to the IP routing table as the best BGP pathway.

The BGP Path Selection Decision Tree

This topic explains how the BGP process evaluates the various attributes to select the best pathway to a destination network.

Route Selection Decision Process

Cisco.com

Consider only (synchronized) routes with no AS loops and a valid next hop, and then:

- Prefer highest weight (local to router)
- Prefer highest local preference (global within AS)
- Prefer route originated by the local router (next hop = 0.0.0.0)
- Prefer shortest AS path
- Prefer lowest origin code (IGP < EGP < incomplete)
- Prefer lowest MED (from other AS)
- Prefer EBGP path over IBGP path
- Prefer the path through the closest IGP neighbor
- Prefer oldest route for EBGP paths
- Prefer the path with the lowest neighbor BGP router ID

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-15

After BGP receives updates about different destinations from different autonomous systems, it decides the best path to choose to reach a specific destination. BGP chooses only a single best path to reach a destination.

The decision process is based on the BGP attributes. When faced with multiple routes to the same destination, BGP chooses the best route for routing traffic toward the destination. BGP considers only (synchronized) routes with no AS loops and a valid next hop. The following process summarizes how BGP chooses the best route on a Cisco router:

- Step 1** If the path is internal and synchronization is on, but the route is not synchronized (not learned via an IGP also), do not consider it.
- Step 2** If the next-hop address of a route is not reachable, do not consider it.
- Step 3** Prefer the route with the highest weight. (Recall that the weight is proprietary to Cisco and is local to the router only.)
- Step 4** If multiple routes have the same weight, prefer the route with the highest local preference. (Recall that the local preference is used within an AS.)
- Step 5** If multiple routes have the same local preference, prefer the route that the local router originated. The locally originated route has a next hop of 0.0.0.0 in the BGP table.
- Step 6** If none of the routes were locally originated, prefer the route with the shortest AS path.

- Step 7** If the AS path length is the same, prefer the lowest origin code (IGP < EGP < incomplete).
- Step 8** If all origin codes are the same, prefer the path with the lowest MED. (Recall that the MED is sent from other autonomous systems.)

The MED comparison is made only if the neighboring AS is the same for all routes considered, unless the **bgp always-compare-med** command is enabled.

Note	The most recent Internet Engineering Task Force (IETF) decision regarding BGP MED assigns a value of infinity to the missing MED, making the route lacking the MED variable the least preferred. The default behavior of BGP routers running Cisco IOS software is to treat routes without the MED attribute as having a MED of 0, making the route lacking the MED variable the most preferred. To configure the router to conform to the IETF standard, use the bgp bestpath missing-as-worst command.
-------------	---

- Step 9** If the routes have the same MED, prefer external paths (EBGP) to internal paths (IBGP).
- Step 10** If synchronization is disabled and only internal paths remain, prefer the path through the closest IGP neighbor. This step means that the router will prefer the shortest internal path within the AS to reach the destination (the shortest path to the BGP next hop).
- Step 11** For EBGP paths, select the oldest route to minimize the effect of routes going up and down (flapping).
- Step 12** Prefer the route with the lowest neighbor BGP router ID value.

Only the best path is entered in the routing table and propagated to the BGP neighbors of the router.

Note	The route selection process summarized here does not cover all cases but is sufficient for a basic understanding of how BGP selects routes.
-------------	---

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Routers send BGP update messages containing attributes to other routers to describe the pathways to the destination networks. Each attribute has characteristics that inform BGP routers receiving updates about how to treat the attribute.
- The AS path attribute is a well-known mandatory attribute that lists the AS numbers that a route has traversed to reach a destination.
- The BGP next-hop attribute is a well-known mandatory attribute that indicates the next-hop IP address to use to reach a destination.
- The local preference attribute is a well-known discretionary attribute that indicates to routers in the AS which path is preferred to exit the AS.
- The MED attribute is an optional nontransitive attribute that indicates to EBGP neighbors the preferred path into an AS.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-16

Summary (Cont.)

Cisco.com

- The origin is a well-known mandatory attribute that defines the origin of the path information.
- The weight attribute is an attribute that Cisco defines for the path selection process. Routes with a higher weight are preferred when multiple routes exist to the same destination.
- BGP follows a multiple-step process when selecting the best route to reach a destination.
- Pathways for a network that are determined not to be the best are eliminated from the selection criteria but are still kept in the BGP forwarding table in case the best path becomes inaccessible.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-17

References

For additional information, refer to these resources:

- RFCs 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, and 2439.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 7-3: Configuring BGP Route Summarization and Examining the BGP Path Selection Process

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 description applies to the AS path attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) optional nontransitive
- Q2) Which description applies to the next-hop attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) optional nontransitive
- Q3) Which description applies to the origin attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) optional nontransitive
- Q4) Which description applies to the local preference attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) optional nontransitive
- Q5) Which description applies to the MED attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) optional nontransitive
- Q6) Which description applies to the weight attribute?
- A) well-known mandatory
 - B) well-known discretionary
 - C) optional transitive
 - D) proprietary to Cisco and not advertised to other BGP routers

- Q7) BGP, by default, will load-balance across how many paths?
- A) 1
 - B) 2
 - C) 4
 - D) 6
- Q8) Which path will BGP prefer when using the weight attribute?
- A) higher weight
 - B) lower weight
- Q9) Which path will BGP prefer when using the local preference attribute?
- A) higher local preference
 - B) lower local preference
- Q10) Which path will BGP prefer when using the MED attribute?
- A) higher MED
 - B) lower MED

Quiz Answer Key

- Q1) A
Relates to: The AS Path Attribute
- Q2) A
Relates to: The Next-Hop Attribute
- Q3) A
Relates to: The Origin Attribute
- Q4) B
Relates to: The Local Preference Attribute
- Q5) D
Relates to: The MED Attribute
- Q6) D
Relates to: The Weight Attribute
- Q7) A
Relates to: BGP Path Selection Criteria
- Q8) A
Relates to: The BGP Path Selection Decision Tree
- Q9) A
Relates to: The BGP Path Selection Decision Tree
- Q10) B
Relates to: The BGP Path Selection Decision Tree

Basic BGP Path Manipulation Using Route Maps

Overview

Knowledge of the behavior of BGP and common configuration options is necessary to configure BGP to exchange information with other autonomous systems. Exchanging updates, where BGP informs an AS of the existence of outside networks, is not the only purpose of BGP. BGP is also implemented to perform PBR.

This lesson discusses manipulating path selection to affect the inbound and outbound traffic policies of an AS. It also discusses how to configure an AS using route maps to manipulate the BGP attributes of local preference and MED to influence BGP path selection.

Relevance

BGP is implemented in internetworks to perform PBR and allow an AS to manipulate the path selection process. This lesson demonstrates how to use route maps with BGP to perform this path manipulation process.

Objectives

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

- Use route maps to set local preference
- Use route maps to set the MED

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Setting Local Preference with Route Maps**
- **Setting the MED with Route Maps**
- **Summary**
- **Quiz**

Setting Local Preference with Route Maps

BGP is designed to perform path manipulation. This topic demonstrates how to use route maps with the BGP local preference attribute to manipulate the best-path decision process. This topic begins with a review of the BGP path selection process.

BGP Is Designed to Implement Policy Routing

Cisco.com

The diagram illustrates a network topology with two Autonomous Systems (ASes): AS 65001 and AS 65004. Router A (in AS 65001) has two outgoing interfaces to router X (in AS 65004). The top interface uses a route map that sets a local preference of 60% Bandwidth Utilization, resulting in 10% Bandwidth Utilization. The bottom interface uses a route map that sets a local preference of 75% Bandwidth Utilization, resulting in 20% Bandwidth Utilization. Router B (in AS 65001) has one outgoing interface to router Y (in AS 65004), which uses a route map that sets a local preference of 20% Bandwidth Utilization, resulting in 75% Bandwidth Utilization. Router X and router Y are shown in a cloud labeled AS 65004.

- BGP is designed for manipulating routing pathways.

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-4

Unlike local routing protocols, BGP was never designed to choose the quickest pathway. BGP was designed to manipulate traffic flow to maximize or minimize bandwidth use. The figure demonstrates a common situation that can result when you are using BGP without any policy manipulation.

Using default settings for path selection in BGP may cause uneven use of bandwidth. In the diagram, router A in AS 65001 is using 60 percent of its outbound bandwidth to router X in AS 65004, but router B is using only 20 percent of its outbound bandwidth. If this utilization is acceptable to the administrator, then no manipulation is needed.

But if the load averages 60 percent and has temporary bursts above 100 percent of the bandwidth, this situation will cause lost packets, higher latency, and higher CPU usage because of the number of packets being routed.

When another link exists to the same locations and is not heavily used, it makes sense to divert some of the traffic to the other pathway. To change outbound path selection from AS 65001, the network administrator must manipulate the local preference attribute.

To determine which path to manipulate, the administrator performs a traffic analysis on Internet-bound traffic by examining the most heavily visited addresses, web pages, or domain names. This information can usually be found by examining network management records or firewall accounting information.

In the example in this figure, for the outbound traffic from AS 65001, 35 percent of all traffic has been heading to www.cisco.com.

The administrator can obtain its address or AS number by performing a reverse Domain Name System (DNS) lookup or by going to www.arin.net and looking up the AS number of Cisco Systems or the address space that is assigned to the company. After this information has been determined, the administrator uses local preference and route maps to manipulate path selection for the Cisco network.

Using a route map, router B can announce all networks that are associated with that AS with a higher local preference than router A announces for those networks. Other routers in AS 65001 running BGP will prefer the routes with the highest local preference. For the Cisco networks, router B announces the highest local preference, so all traffic destined for that AS will exit AS 65001 via router B.

The outbound load for router B increases from its previous load of 20 percent to 35 percent to account for the extra traffic from AS 65001 destined for Cisco networks. The outbound load for router A, which was originally 60 percent, should decrease, and this change will bring the outbound load on both links into a relative balance.

Just as there was a loading issue outbound from AS 65001, there can be a similar problem inbound. Maybe the sales web servers are located on the same subnet behind router B, causing the inbound load for router B to average higher utilization.

To manipulate how traffic enters an AS, use the BGP MED attribute. AS 65001 announces a lower MED for network 192.168.25.0/24 to AS 65004 out router A. This MED is a recommendation to the next AS on how to enter into AS 65001. However, the MED is not considered until Step 6 of the BGP path selection process. If AS 65004 prefers to keep its AS path via router Y to router B in AS 65001, then AS 65004 simply needs to have router Y announce a higher local preference to the BGP routers in AS 65004 for network 192.168.25.0/24 than router X announces.

The local preference that router Y advertises to other BGP routers in AS 65004 is evaluated before the MED coming from router A in AS 65001. MED is considered a recommendation because the receiving AS can override it by having that AS manipulate a value before the MED is considered.

In the figure, 55 percent of all traffic is going to the 192.168.25.0/24 subnet (router A). The inbound utilization to router A is averaging only 10 percent, but the inbound utilization to router B is averaging 75 percent. If AS 65001 were set to prefer to have all traffic going to 192.168.25.0/24 to enter through router A from AS 65004, the load inbound on router A would increase and the load inbound on router B would decrease.

The problem is that if the inbound load for router A spikes to more than 100 percent and causes the link to cycle, all the sessions crossing that link could be lost. If these sessions were purchases being made on AS 65001 web servers, revenue would be lost, which is something administrators want to avoid at all costs.

If the load averages below 50 percent for the outbound or inbound case, path manipulation might not be needed. However, when a link starts to spike up to the capacity of the link for an extended period of time, more bandwidth is needed or path manipulation should be considered.

Route Selection Decision Process

Cisco.com

Consider only synchronized routes with no AS loops and a valid next hop, and then:

- Step 1: Prefer highest weight (local to router)**
- Step 2: Prefer highest local preference (global within AS)**
- Step 3: Prefer route originated by the local router**
- Step 4: Prefer shortest AS path**
- Step 5: Prefer lowest origin code (IGP < EGP < incomplete)**
- Step 6: Prefer lowest MED (from other AS)**
- Step 7: Prefer EBGP path over IBGP path**
- Step 8: Prefer the path through the closest IGP neighbor**
- Step 9: Prefer oldest route for EBGP paths**
- Step 10: Prefer the path with the lowest neighbor BGP router ID**

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 7-5

An AS rarely implements BGP with only one EBGP connection. This situation generally means that multiple pathways exist for each network in the BGP forwarding database. If only one pathway exists and it is loop-free and synchronized with the IGP for IBGP, and the next hop is reachable, the pathway is submitted to the IP routing table.

There is no path selection taking place because there is only one path and manipulating it will derive no benefit. This situation is considered Step 0, and it is not a common reason to select a BGP pathway because multiple pathways usually exist for each network in the BGP forwarding database.

The BGP route selection decision process involves a series of 10 steps.

Step 1 looks at weight, which is by default set to 0 for nonoriginated routes.

Step 2 compares local preference, which by default is set to 100 for all networks. Both of these steps have an effect only if the network administrator executes path manipulation, for example, by using a route map to set the local preference or weight to some nondefault value, which causes path manipulation.

Step 3 looks at networks that are owned by this AS. If one of the routes is injected into the BGP table by the local router, the local router prefers it to any routes that are received from other BGP routers.

Step 4 selects the pathway that has the least number of autonomous systems to cross. This is the most common reason that a pathway is selected in BGP.

If a network administrator does not like the path with the least number of autonomous systems in it, the administrator needs to manipulate weight or local preference to change which outbound path that BGP will choose.

Step 5 looks at how a network was introduced into BGP. This introduction is usually either with network statements (“i” for an origin code) or through redistribution (“?” for an origin code).

Step 6 looks at the MED to judge where the other AS prefers this AS as an entry point to reach a given network. Cisco sets the MED to 0 by default. The MED does not participate in path selection unless the network administrator of the other AS decides to manipulate the pathways using the MED.

If multiple pathways exist with the same number of autonomous systems to traverse, the next most common decision point is Step 7, which states that an externally learned path from an EBGP neighbor is preferred over a pathway cross-learned from an IBGP neighbor.

A router in an AS would prefer to use the bandwidth of the ISP to reach that network as opposed to using internal bandwidth to reach an IBGP neighbor on the other side of its network. This situation is probably the second most common reason for default path selection.

If the AS path is equal and the router in an AS has no EBGP neighbors for that network, just IBGP neighbors, it makes sense to take the quickest pathway to the nearest exit point.

Step 8 looks for the closest IBGP neighbor using the local routing protocol to decide the meaning of closest (for example, RIP uses hop count and OSPF uses least cost based on bandwidth).

If the AS path is equal and it is equal cost to any IBGP neighbor, or all neighbors for this network are EBGP, step 9—use the oldest pathway—is a common reason for selecting one pathway over another. EBGP neighbors rarely establish sessions at the exact same time. One session is likely older than another, so the pathways through that neighbor are more stable because they have been up longer.

If all of the above are equal, the next most common decision is to take the neighbor with the lowest BGP router ID, which is the final decision-making step, Step 10.

BGP Local Preference

Cisco.com

Local preference is used in the following ways:

- Within an AS between IBGP speakers
- To determine the best pathway to exit the AS to reach an outside network
- Set to 100 by default; higher values are preferred

Router(config-router)#

bgp default local-preference value

- Changes the default local preference value
- All routes advertised to an IBGP neighbor are set to the value specified using this command

© 2004 Cisco Systems, Inc. All rights reserved.

BSGI 2.1 7-6

Local preference is used only within an AS between IBGP speakers to determine the best pathway to leave the AS to reach an outside network.

The metric is set to 100 by default; higher values are preferred. With the command that is shown in the figure, all IBGP routes that are advertised are set to the value specified.

If an EBGP neighbor receives a local preference value, the EBGP neighbor ignores it.

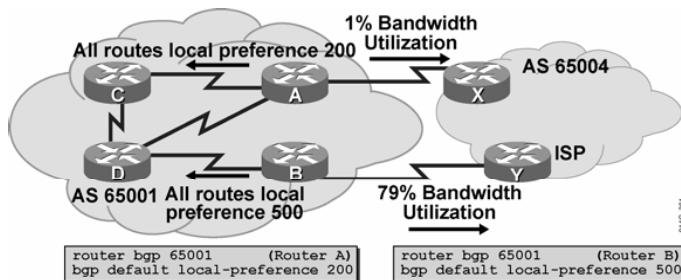
The **bgp default local-preference** command changes the default local preference value.

Table 1: The bgp default local-preference Command Parameters

Parameter	Description
value	Local preference value from 0 to 4294967295. Higher is more preferred.

Setting a Default Local Preference

Cisco.com



- All routers are running BGP.
- Router B is announcing local preference of 500 for all routes.
- Router A is announcing local preference of 200 for all routes.
- BGP path selection chooses Step 2 for all routes causing all traffic to exit through router B, which was not the intention.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-7

Manipulating the default local preference can have an immediate and dramatic effect on traffic flow leaving an AS. Before making any changes to manipulate pathways, the network administrator should perform a thorough traffic analysis to understand the effects of the change.

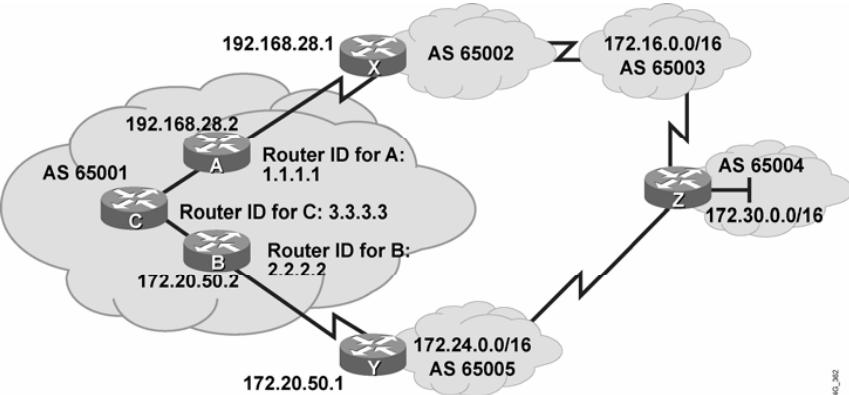
In the diagram, the network administrator changed the default local preference to 500 on router B for all routes and to 200 on router A.

As a result of the change, all BGP routers in AS 65001 send all traffic that is destined for the Internet to router B, causing its outbound utilization to be much higher and the utilization out router A to be reduced to a minimal amount.

This change is probably not what the network administrator intended. Instead, the network administrator should use route maps to set certain networks to have a higher local preference through router B to decrease some of the original outbound load that was being sent out on router A.

Local Preference Case Study

Cisco.com



What is the best path for router C to 65003, 65004, and 65005?

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

The figure demonstrates the manipulation of local preference using route maps in AS 65001.

From router C in AS 65001, the best path to AS 65003, 65004, and 65005 is determined in the following way:

Steps 1 and 2 look at weight and local preference and use the default settings of weight equals 0 and local preference equals 100 for all routes that are learned from the IBGP neighbors of A and B.

Step 3 does not help decide the best pathway because the three AS routes are not owned or originated by AS 65001.

Step 4 prefers the shortest AS path; the options are two autonomous systems (65002, 65003) through router A or three autonomous systems through IBGP neighbor router B (65005, 65004, 65003). Therefore, the shortest AS path from router C to AS 65003 is through router A.

The best pathway from router C to networks in AS 65005 is also selected by Step 4, shortest AS path. The shortest path from router C to AS 65005 is through router B because it is one AS (65005) compared to four autonomous systems (65002, 65003, 65004, 65005) through router A.

The best pathway from router C to networks in AS 65004 is also selected by Step 4, shortest AS path. The shortest path from router C to AS 65004 is through router B because it is two autonomous systems (65005, 65004) as compared to three autonomous systems (65002, 65003, 65004) through router A.

Default Settings on Router C

Cisco.com

RouterC# show ip bgp

```
BGP table version is 7, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop        Metric LocPrf Weight Path
* 172.16.0.0        172.20.50.1    100    0 65005 65004 65003 i
* >i               192.168.28.1    100    0 65002 65003 i
* >i 172.24.0.0      172.20.50.1    100    0 65005 i
* i                192.168.28.1    100    0 65002 65003 65004 65005 i
* >i 172.30.0.0      172.20.50.1    100    0 65005 65004 i
* i                192.168.28.1    100    0 65002 65003 65004i
```

By default, BGP selects the shortest AS path as the best (>) pathway.

In AS 65001, the percent of traffic going to 172.24.0.0 is 30%, 172.30.0.0 is 20%, and 172.16.0.0 is 10%.

50% of all traffic will go to the next hop of 172.20.50.1 (AS 65005), and 10% of all traffic will go to the next hop of 192.168.28.1 (AS 65002).

Make traffic to 172.30.0.0 select the next hop of 192.168.28.1 to achieve load sharing where both external links get approximately 30% of the load.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-9

The diagram demonstrates the BGP forwarding table on router C in AS 65001 with only default settings for BGP path selection. The diagram shows only those networks of interest to this example:

- 172.16.0.0 in AS 65003
- 172.24.0.0 in AS 65005
- 172.30.0.0 in AS 65004

Each network has two pathways that are loop-free and synchronization-disabled, and have a valid next-hop address. All routes have a weight of 0 and a default local preference of 100, thus Steps 1 and 2 in the BGP path selection process are equal.

This router did not originate any of the routes (Step 3), so Step 4 instructs BGP to choose the shortest AS path.

For network 172.16.0.0, the shortest AS path of two autonomous systems (65002, 65003) is through the next hop of 192.168.28.1.

For network 172.24.0.0, the shortest AS path of one AS (65005) is through the next hop of 172.20.50.1.

For network 172.30.0.0, the shortest AS path of two autonomous systems (65005, 65004) is through the next hop of 172.20.50.1.

Both router A and B are not using the **next-hop-self** option in this example.

A traffic analysis reveals that the link going through router B to 172.20.50.1 is heavily used, and the link through router A to 192.168.28.1 is hardly used at all.

The three largest-volume destination networks on the Internet from AS 65001 are 172.30.0.0, 172.24.0.0, and 172.16.0.0.

This analysis reveals that 30 percent of all Internet traffic is going to network 172.24.0.0 (via router B); 20 percent is going to network 172.30.0.0 (via router B); and 10 percent is going to network 172.16.0.0 (via router A).

Therefore, only 10 percent of all traffic is using the link out of router A to 192.168.28.1, and 50 percent of all traffic is using the link out of router B to 172.20.50.1.

The network administrator has decided to divert traffic to network 172.30.0.0 and send it out router A to the next hop of 192.168.28.1, so that the loading between routers A and B is more balanced.

Route Map for Router A

Cisco.com

```
Router A's Configuration:  
router bgp 65001  
neighbor 2.2.2.2 remote-as 65001  
neighbor 3.3.3.3 remote-as 65001  
neighbor 2.2.2.2 remote-as 65001 update-source loopback0  
neighbor 3.3.3.3 remote-as 65001 update-source loopback0  
neighbor 192.168.28.1 remote-as 65002  
neighbor 192.168.28.1 route-map local_pref in  
'  
route-map local_pref permit 10  
match ip address 65  
set local-preference 400  
'  
route-map local_pref permit 20  
'  
access-list 65 permit 172.30.0.0 0.0.255.255
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-10

The figure demonstrates the use of a route map on router A to alter the network 172.30.0.0 BGP update from router X (192.168.28.1) to have a high local preference value of 400 so that it will be more preferred.

The first line of the route map is a permit statement with a sequence number of 10 for a route map called local_pref. The match condition for that line is checking all networks that are permitted by access list 65. Access list 65 permits all networks that start with the first two octets of 172.30.0.0 and sets those networks to a local preference of 400.

The second line of the route map is a permit statement with a sequence number of 20 for the route map called local_pref, but it does not have any match or set statements. This statement is a permit all statement for route maps.

Because you do not try to match any fields for the remaining networks, they are all permitted with their current settings. In this case, the local preference for network 172.16.0.0 and 172.24.0.0 stays set at the default of 100. The sequence of 20 is chosen for the second statement in case other policies at a later date have to be implemented before the permit all statement.

This route map is linked to neighbor 192.168.28.1 as an inbound route map. Therefore, as router A receives updates from 192.168.28.1, it processes them through the local_pref route map and sets the local preference accordingly as the networks are placed into the BGP forwarding table of router A.

Local Preference Learned by Router C

Cisco.com

RouterC# show ip bgp

```
BGP table version is 7, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop        Metric LocPrf Weight Path
* 172.16.0.0     172.20.50.1    100    0 65005 65004 65003 i
*>i             192.168.28.1    100    0 65002 65003 i
*>i 172.24.0.0   172.20.50.1    100    0 65005 i
* i              192.168.28.1    100    0 65002 65003 65004 65005 i
* 172.30.0.0     172.20.50.1    100    0 65005 65004 i
*>i             192.168.28.1    400    0 65002 65003 650041
```

- Best (>) pathways for networks 172.16.0.0/16 and 172.24.0.0/16 have not changed.
- Best (>) pathway for network 172.30.0.0 has changed to a new next hop of 192.168.28.1 due to the next hop of 192.168.28.1 having a higher local preference, 400.
- In AS 65001, the percentage of traffic going to 172.24.0.0 is 30%, 172.30.0.0 is 20%, and 172.16.0.0 is 10%.
- 30% of all traffic will go to the next hop of 172.20.50.1 (AS 65005), and 30% of all traffic will go to the next hop of 192.168.28.1 (AS 65002).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-11

Examining the BGP forwarding table on router C in AS 65001 after the BGP session has been reset shows that router C has learned about the new local preference value (400) coming from router A for network 172.30.0.0.

The only difference in this table as compared to the original display that did not have local preference manipulation is that network 172.30.0.0 is now choosing to go to a network hop of 192.168.28.1 because its local preference of 400 is higher than the local preference of 100 for the next hop of 172.20.50.1.

The AS path through 172.20.50.1 is still shorter than the pathway through 192.168.28.1, but AS path length is not evaluated until Step 4, whereas local preference was examined in Step 2. Therefore, the higher local preference path was chosen as the best pathway.

Setting the MED with Route Maps

This topic demonstrates how an administrator can use route maps with the MED attribute to manipulate the path decision process.

BGP Multi-Exit Discriminator: Inbound Metric

Cisco.com

- MED is used when multiple pathways exist between two autonomous systems.
- A lower MED value is preferred.
- The default setting for Cisco is MED = 0.
- The metric is nontransitive.
- By default, MED is shared only between two autonomous systems that have multiple EBGP connections with each other.

Router(config-router)#

default-metric number

- MED is considered the metric of BGP.
- All routes that are advertised to an EBGP neighbor are set to the value specified using this command.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-12

The MED is used only when two autonomous systems exchange BGP routing information with each other. If an AS connects to two different ISPs and passes the ISPs a MED value for its network, when either ISP announces the network of the first AS to the other ISP (or any other AS for that matter), the latter ISP will reset the MED value to $2^{32} - 1$.

The MED is used to decide how to enter an AS. It is used when multiple pathways exist between two autonomous systems, and one AS is trying to influence the incoming path from the other AS.

Because the MED is evaluated late in the BGP path selection process (Step 6), it usually has no influence on the BGP selection process. For example, an AS receiving a MED for a route can change its local preference to enable the AS to override what the other AS is advertising with its MED value.

When BGP is comparing MED values for the same destination network in the path selection process, the lowest MED value is preferred.

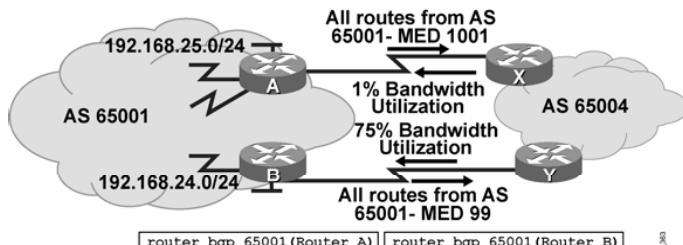
The default MED value for each network that an AS owns and advertises to an EBGP neighbor is set to 0. To change this value, use the **default-metric number** command under the BGP process.

Table 2: The default-metric Command Parameters

Parameter	Description
<i>number</i>	(Optional) The value of the metric, which for BGP is the MED.

BGP Using the Default MED

Cisco.com



- Router B is announcing a MED of 99 for routes originating in AS 65001.
- Router A is announcing a MED of 1001 for routes originating in AS 65001.
- If AS 65004 does not have any overriding policy, it will choose router Y as its exit point to get to all networks in AS 65001 because of Step 6: prefer lowest MED (from other AS).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-13

In the figure, AS 65001 tries to manipulate how AS 65004 chooses its pathway to reach routes in AS 65001. By changing the default metric under the BGP process on router A to 1001, router A advertises a MED of 1001 for all routes to router X. Router X then informs all the other routers in AS 65004 of the MED through router X to reach networks originating in AS 65001. A similar event is happening on router B, but router B is advertising a MED of 99 for all routes to router Y. All routers in AS 65004 see a MED of 1001 through the next hop of A and a MED of 99 through the next hop of B to reach networks in AS 65001.

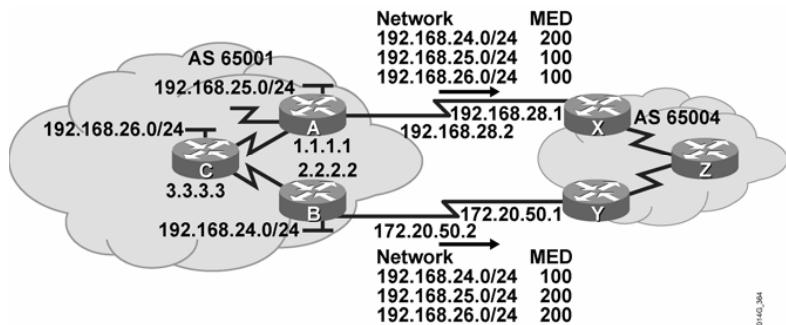
The **next-hop-self** option is not used at router X or Y. If AS 65004 has no overriding policy, all routers in AS 65004 will choose to exit their AS through router Y and enter AS 65001 through router B. This selection causes the inbound bandwidth utilization of router A to decrease to almost nothing except for BGP routing updates, and it causes the inbound utilization on router B to increase and account for all returning packets from the Internet to AS 65001.

Manipulating the default MED value can have an immediate and dramatic effect on traffic flow entering your AS. Before making any changes to manipulate pathways, you should perform a thorough traffic analysis to ensure that you understand the effects of the change.

In this figure, the network administrator changed the default MED to 99 on router B for all routes and to 1001 on router A, causing all inbound traffic to enter through router B. This situation is probably not what the network administrator intended. Instead, to load-share the inbound traffic to AS 65001, the AS 65001 network administrator should set certain networks to have a lower MED through router B and other networks to have a lower MED through router A. Route maps should be used to set the appropriate MED values for various networks.

BGP Using Route Maps and the MED

Cisco.com



© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-14

The figure is used in the following configurations to demonstrate how to manipulate inbound traffic using route maps and the BGP MED attribute.

The intention of these route maps is to designate router A as the preferred pathway to reach networks 192.168.25.0/24 and 192.168.26.0/24, and router B as the preferred pathway to reach network 192.168.24.0/24.

The other networks should still be reachable through each router in case of a link or router failure.

Route Map for Router A

Cisco.com

```
Router A's Configuration:  
router bgp 65001  
neighbor 2.2.2.2 remote-as 65001  
neighbor 3.3.3.3 remote-as 65001  
neighbor 2.2.2.2 update-source loopback0  
neighbor 3.3.3.3 update-source loopback0  
neighbor 192.168.28.1 remote-as 65004  
neighbor 192.168.28.1 route-map med_65004 out  
!  
route-map med_65004 permit 10  
match ip address 66  
set metric 100  
route-map med_65004 permit 100  
set metric 200  
!  
access-list 66 permit 192.168.25.0.0 0.0.0.255  
access-list 66 permit 192.168.26.0.0 0.0.0.255
```

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-15

The MED is set outbound when a router is advertising to an EBGP neighbor. In the configuration example for router A, a route map named med_65004 is linked to neighbor 192.168.28.1 as an outbound route map.

When router A sends an update to neighbor 192.168.28.1, it will process the outbound update through route map med_65004 and use a set statement to change any values that are specified, as long as the preceding match statement is met in that section of the route map.

The first line of the route map is a permit statement with a sequence number of 10 for a route map called med_65004. The match condition for that line checks all networks that are permitted by access list 66. The first line of access list 66 permits any networks that start with the first three octets of 192.168.25.0, and the second line of access list 66 permits networks that start with the first three octets of 192.168.26.0.

Any networks that are permitted by either of these lines are set to a MED of 100. All other networks are not permitted by this access list, so they are not set to a MED of 100. (There is an “implicit deny all” at the end of all access lists.) These other networks must proceed to the next route map statement in the med_65004 route map.

The second line of the route map is a permit statement with a sequence number of 100 for the route map called med_65004. The route map does not have any match statements, just a set metric 200 statement. This statement is a permit all statement for route maps.

Because the network administrator does not specify a match condition for this portion of the route map, all networks being processed through this section of the route map (sequence number 100) are permitted, but they are set to a MED of 200. If the network administrator did not set the MED to 200, by default it would have been set to a MED of 0. Because 0 is less than 100, the routes with a MED of 0 would have been the preferred pathways to the networks in AS 65004.

Route Map for Router B

Cisco.com

```
Router B's Configuration:  
router bgp 65001  
neighbor 1.1.1.1 remote-as 65001  
neighbor 3.3.3.3 remote-as 65001  
neighbor 1.1.1.1 update-source loopback0  
neighbor 3.3.3.3 update-source loopback0  
neighbor 172.20.50.1 remote-as 65004  
neighbor 172.20.50.1 route-map med_65004 out  
  
route-map med_65004 permit 10  
match ip address 66  
set metric 100  
route-map med_65004 permit 100  
set metric 200  
  
access-list 66 permit 192.168.24.0 0.0.0.255
```

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-16

The MED is set outbound when advertising to an EBGP neighbor. In the configuration example for router B, a route map named med_65004 is linked to neighbor 172.20.50.1 as an outbound route map.

Before router B sends an update to neighbor 172.20.50.1, it will process the outbound update through route map med_65004 and use a set statement to change any values that are specified, as long as the preceding match statement is met in that section of the route map.

The first line of the route map is a permit statement with a sequence number of 10 for a route map called med_65004. The match condition for that line is checking all networks that are permitted by access list 66. Access list 66 on router B permits any networks that start with the first three octets of 192.168.24.0.

Any networks that are permitted by this line are set to a MED of 100. All other networks are not permitted by this access list, so they are not set to a MED of 100. These other networks must proceed to the next route map statement in the med_65004 route map.

The second line of the route map is a permit statement with a sequence number of 100 for the route map called med_65004, but it does not have any match statements, just a set metric 200 statement. This statement is a permit all statement for route maps.

Because the network administrator does not specify a match condition for this portion of the route map, all networks being processed through this topic are permitted, but they are set to a MED of 200.

If the network administrator did not set the MED to 200, by default it would have been set to a MED of 0. Because 0 is less than 100, the routes with a MED of 0 would have been the preferred pathways to the networks in AS 65004.

MED Learned by Router Z

Cisco.com

```
RouterZ# show ip bgp
```

```
BGP table version is 7, local router ID is 122.30.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop        Metric LocPrf Weight Path
*->i192.168.24.0    172.20.50.2    100    100      0 65001 i
*     i               192.168.28.2    200    100      0 65001 i
*     i192.168.25.0    172.20.50.2    200    100      0 65001 i
*>i     192.168.28.2    100    100      0 65001 i
*     i192.168.26.0    172.20.50.2    200    100      0 65001 i
*>i     192.168.28.2    100    100      0 65001 i
```

- Examine the networks that have been learned from AS 65001 on Router Z in AS 65004.
- For all networks: Weight is equal (0); local preference is equal (100); routes are not originated in this AS; AS path is equal (65001); origin code is equal (i).
- 192.168.24.0 has a lower metric (MED) through 172.20.50.2 (100) than 192.168.28.2 (200).
- 192.168.25.0 has a lower metric (MED) through 192.168.28.2 (100) than 172.20.50.2 (200).
- 192.168.26.0 has a lower metric (MED) through 192.168.28.2 (100) than 172.20.50.2 (200).

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-17

The BGP forwarding table on router Z in AS 65004 displays the networks that have been learned from AS 65001. Other networks that do not affect this example have been omitted.

On router Z, there are multiple pathways to reach each network. These pathways all have valid next-hop addresses and synchronization disabled, and are loop-free, so the conditions for Step 0 are met. All networks have a weight of 0 and a local preference of 100, so Steps 1 and 2 are equal.

None of the routes were originated by this router or any router in AS 65004. All networks came from AS 65001, so Step 3 does not apply. All networks have an AS path of one AS (65001) and were introduced into BGP with network statements ("i" is the origin code), so Steps 4 and 5 are equal.

Step 6 states that BGP chooses the lowest MED if all preceding steps are equal or do not apply.

For network 192.168.24.0, the next hop of 172.20.50.2 has a lower MED than the next hop of 192.168.28.2. Therefore, for network 192.168.24.0, the pathway through 172.20.50.2 is the preferred pathway.

For networks 192.168.25.0 and 192.168.26.0, the next hop of 192.168.28.2 has a lower MED of 100 as compared to the MED of 200 through the next hop of 172.20.50.2. Therefore, 192.168.28.2 is the preferred pathway for those networks.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Route maps can be used with the BGP local preference attribute to manipulate the best-path decision process. When you are using route maps to set local preference:**
 - Higher local preference values are preferred.
 - Local preference is used only between IBGP speakers within the same AS.
- **Route maps can be used with MED values to manipulate packets returning to an AS. When you are using route maps to set the MED:**
 - Lower MED values are preferred.
 - The MED is used only between EBGP neighbors.

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 statements are true when you are using route maps to set local preference?
(Choose two.)
- A) The higher value for local preference is preferred.
 - B) Local preference is used only between EBGP neighbors.
 - C) The lower value for local preference is preferred.
 - D) Local preference is used only between IBGP neighbors.
- Q2) Which two statements are true when you are using route maps to set the MED?
(Choose two.)
- A) The higher value for the MED is preferred.
 - B) The MED is used between EBGP neighbors only.
 - C) The lower value for the MED is preferred.
 - D) The MED is used between IBGP neighbors only.

Quiz Answer Key

Q1) A, D

Relates to: Setting Local Preference with Route Maps

Q2) B, C

Relates to: Setting the MED with Route Maps

Design Options for Multihoming

Overview

When you are connecting to multiple ISPs, there are three options to consider. A customer may take default routes from all providers and pass them to its internal routers. A customer may also take a partial routing table from all providers and redistribute the table into its internal routing protocol, or take the full Internet routing table and run Border Gateway Protocol (BGP) on the core routers of the network. These options are discussed in this lesson, including their benefits and drawbacks.

Relevance

The Internet has become a profitable and indispensable tool for the day-to-day operations of many companies; therefore, these companies need robust connectivity to ensure Internet availability. To accomplish continuous Internet connectivity, you need to understand various design options. This lesson discusses these options so you can choose the appropriate type of connectivity.

Objectives

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

- List three design options that are used to manipulate path selection when you are multihoming in BGP
- Describe the benefits of receiving a default route from each provider and passing it to internal routers
- Identify the benefits of receiving a partial routing table from each provider
- Identify the benefits of receiving the full Internet routing table from each provider and configuring BGP on internal routers

Learner Skills and Knowledge

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

- Cisco CCNA® certification or equivalent knowledge and experience
- Knowledge of routing protocol operation and configuration for Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) single-area networks

Outline

The outline lists the topics included in this lesson.

Outline

Cisco.com

- **Overview**
- **Design Choices with Multihoming for BGP**
- **Default Route from Each Provider**
- **Partial Routing Table from Each Provider**
- **Full Routing Table from Each Provider**
- **Summary**
- **Quiz**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-3

Design Choices with Multihoming for BGP

This topic discusses the benefits of BGP multihoming and lists the three design options that are available to implement multihoming.

What Is Multihoming?

Cisco.com

Connecting to two or more ISPs to increase the following:

- **Reliability—If one ISP or connection fails, there is still Internet access.**
- **Performance—Better path selection to common Internet destinations.**

© 2004 Cisco Systems, Inc. All rights reserved.
BSCI 2.1 7-4

Multihoming describes a situation where an AS connects to more than one ISP. Two typical reasons for multihoming are as follows:

- **To increase the reliability of the connection to the Internet:** If one connection fails, the other connection remains available.
- **To increase the performance of the connection:** You can use better paths to certain destinations.

If a company has only a single link to the Internet, BGP is inappropriate and a default route is the recommended design. When you are using a single connection and all packets go out the same interface to the ISP, the overhead of BGP does not provide enough benefits to warrant its use.

The benefits of BGP are apparent when an AS has multiple EBGP connections to either a single AS or multiple autonomous systems. Having multiple connections allows an organization to have redundant connections to the Internet so that if a single pathway becomes unavailable, connectivity can still be maintained.

A drawback to having all of your EBGP connections to a single ISP is that connectivity issues in that single ISP could cause your AS to lose connectivity to the Internet.

By having connections to multiple ISPs, an AS gains the following benefits:

- Has redundancy with the multiple connections
- Is not tied into the routing policy of a single ISP
- Has more pathways to the same networks for better policy manipulation

Types of Connectivity

Cisco.com

Following are three common ways to configure the connections:

- **Default routes from all providers**
 - Pass default route to internal routers
- **Provider-owned routes and the default route from each provider**
 - Redistribute into Interior Gateway Protocol (IGP) for internal routers, or
 - Run BGP on all routers in the AS
- **Full routes from all providers**
 - Run BGP on all internal routers; turn off BGP synchronization

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

If an organization has determined that it will perform multihoming with BGP, there are three design options for implementing this decision. The configuration of multihoming to different ISPs can be classified depending on the routes that are provided to the AS from the ISPs.

Three common ways to configure multihoming are as follows:

- Each ISP passes only a default route to the AS.
- Each ISP passes only a default route and selected specific routes to the connecting AS.
- Each ISP passes all routes to the AS.

Default Route from Each Provider

Your first design choice for multihoming is to receive only a default route from each ISP. This topic describes the benefits and important considerations of receiving only a default route from each provider and passing it to internal routers.

Default Routes from All Providers

Cisco.com

- **Low memory and CPU usage**
- **ISPs send BGP default route**
 - Default route passed into IGP
 - Choice of exit point when multiple default routes exist will be lowest IGP metric
- **The AS of the customer sends all of its routes to ISPs**
- **Inbound path to the AS of the customer is decided by the ISPs**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-6

In this design choice, all ISPs pass only default routes to the AS. This configuration requires the least resources within the AS because a default route is used to reach any external destinations. The AS sends all its routes to the ISPs, which process and pass them on to other autonomous systems.

If a router in the AS learns about multiple default routes, the local interior routing protocol installs the best default route into the routing table. From the perspective of this router, it takes the default route with the least-cost IGP metric.

This IGP default route will route packets destined to the external networks to an edge router of this AS, which is running EBGP with the ISPs. The edge router will use the BGP default route to reach all external networks.

The route that inbound packets take to reach the AS is decided outside the AS (within the ISPs and other autonomous systems).

Regional ISPs that have multiple connections to national or international ISPs commonly implement this option. The regional ISPs do not use BGP for path manipulation; however, they require the capability of adding new customers as well as the networks of the customers.

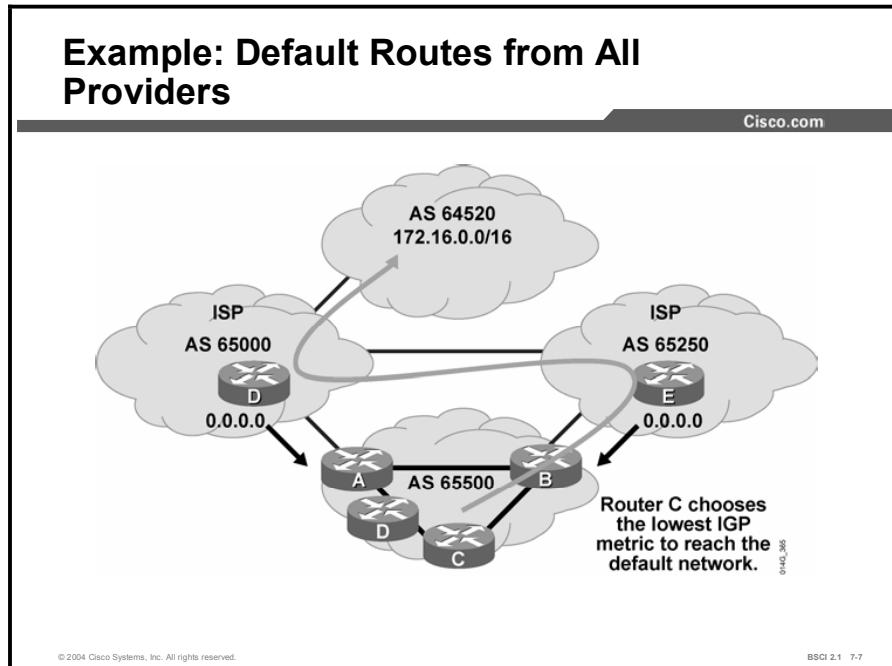
If the regional ISP does not use BGP, then each time that the regional ISP adds a new set of networks, the customers must wait until the national ISPs add these networks to their BGP process and place static routes pointing at the regional ISP.

By running EBGP with the national or international ISPs, the regional ISP needs to add only the new networks of the customers to its BGP process. These new networks automatically propagate across the Internet with minimal delay.

When a customer chooses to receive default routes from all providers, it must understand the following limitations of this option:

- Path manipulation cannot be performed because only a single route is being received from each ISP.
- Bandwidth manipulation is extremely difficult and can be accomplished only by manipulating the IGP metric of the default route.
- Diverting some of the traffic from one exit point to another is challenging because all destinations are using the same default route for path selection.

Example



In this figure, AS 65000 and AS 65250 send default routes into AS 65500. The ISP that a specific router within AS 65500 uses to reach any external address is decided by the IGP metric that is used to reach the default route within the AS.

For example, if you use RIP within AS 65500, router C selects the route with the lowest hop count to the default route when sending packets to network 172.16.0.0.

Partial Routing Table from Each Provider

This topic examines receiving a partial BGP table from each ISP and either redistributing BGP into the IGP or running BGP on internal routers in the AS. This topic also discusses the benefits and limitations of this approach.

Provider-Owned Routes and the Default Route from Each Provider

Cisco.com

- **Medium memory and CPU usage**
- **Best path to ISP-owned networks and to customer-specified networks is usually the shortest AS path**
- **Have ability to override path choice for some networks**
- **IGP metric to default route used for all other destinations**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-8

In the second design option for multihoming, all ISPs pass default routes plus select specific routes to the AS.

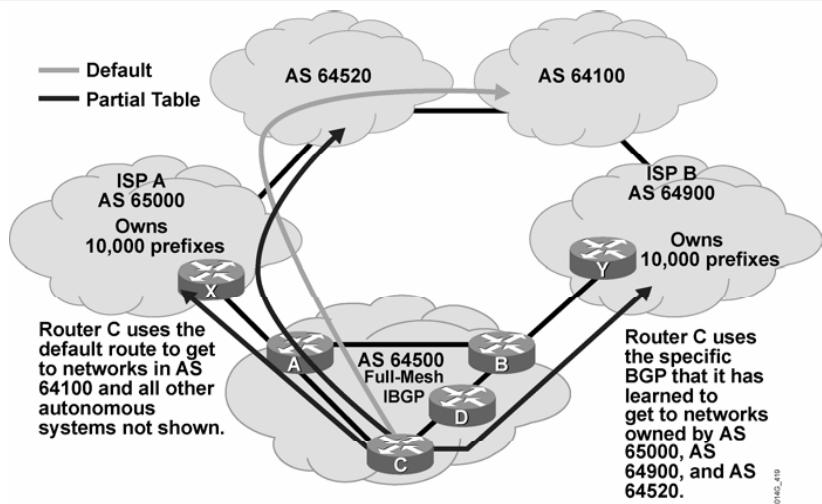
A customer running EBGP with an ISP that wants a partial routing table generally receives the networks that the ISP and its other customers own. The customer can also receive the routes from any other AS that the customer desires, in other words, receive customer-specified routes and networks.

Major ISPs are assigned between 2000 and 10,000 CIDR blocks of IP addresses from the IANA. An ISP reassigns this address space to its customers.

If the ISP passes this information to a customer that wants only a partial BGP routing table, the customer can redistribute these routes into its IGP. The internal routers of the customer (these routers are not running BGP) can then receive these routes via redistribution. They can take the nearest exit point based upon the best metric of specific networks instead of taking the nearest exit point based on the default route.

Default Routes from All Providers and Partial Table

Cisco.com



Acquiring a partial BGP table from each provider is beneficial because path selection for outbound and inbound traffic will be more predictable than using a default route.

If the internal routers of an AS receive only a default route and are closer to ISP A than ISP B, all packets with a destination address outside this AS go to ISP A. ISP A forwards the packets to the rest of the Internet, including the networks that are owned by ISP B. Taking the pathway through ISP A to reach the AS of ISP B is a longer AS path than going directly to ISP B.

ISP B must return the packets to the originating AS. ISP B has a direct connection to that AS or can take a roundabout pathway back through ISP A. Sending the packet directly to the originating AS means the packet enters the AS at a different point than it exited the AS.

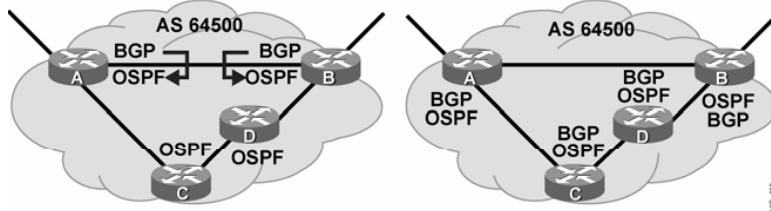
In this figure, AS 65000 and AS 64900 send default routes and the routes that each ISP owns to AS 64500. AS 65000 and AS 64900 also send specific routes to the customer network (AS 64520 in this example) to AS 64500. The customer (AS 64500) asks both providers to pass networks from AS 64520 (customer-specified AS or networks) due to the amount of traffic between AS 64520 and AS 64500.

By running IBGP between the internal routers within AS 64500, the ISP that a specific router within AS 64500 uses to reach the customer networks (AS 64520 in this case) is usually the shortest AS path. The shortest AS path to AS 64520 is via AS 65000 through router A.

The routes to AS 64100 and to other autonomous systems not shown in the figure that are not specifically advertised to AS 64500 by ISP A and ISP B are decided by the IGP metric that is used to reach the default route within the AS.

Partial Table: Redistribute into IGP or Run BGP on Internal Routers

Cisco.com



- **BGP redistributed into IGP (not recommended):**
 - Use IGP metric to exit AS for specific routes.
 - Only administrators of edge routers need to understand BGP.
- **Partial table from ISP and BGP running on all internal routers (recommended):**
 - Path manipulation is easier using BGP attributes.
 - Router configuration is more complex.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-10

This configuration requires more resources within the AS than just passing the default route to this AS because all external routes must be processed. BGP sends all of routes for the AS to the ISPs, which process and pass them to other autonomous systems. By limiting the size of the BGP update that is received from each ISP and not running BGP on the internal routers in the AS, this option proves to be less CPU- and bandwidth-intensive than receiving the full BGP table and running BGP on all internal routers.

An AS that is receiving a partial Internet routing table has two choices for internal routers to reach networks outside its AS. The first choice is to use redistribution of BGP into the internal routing protocol. The AS can take the limited amount of BGP and redistribute it into the local routing protocol. If this option is used, internal routers will use the IGP metric of the redistributed routes to decide the best way to exit the autonomous system.

The path to all other external destinations that are not explicitly known through redistribution is decided by the IGP metric that is used to reach the default route within the AS.

Another choice besides redistributing the limited amount of BGP into the IGP is to run BGP on at least the core routers, if not all routers, in the AS. This choice allows the BGP administrator the ability to more easily manipulate the path selection process than when using just the IGP routing metric. Local preference can be used on a per-network basis as opposed to manipulating the bandwidth statement or interface cost for OSPF or EIGRP. In IGPs like OSPF, manipulating individual routes can be difficult because best paths are chosen based upon the least-cost bandwidth for an interface that will apply to all networks using that pathway. Changing the bandwidth or interface cost to affect how another router chooses the best pathway for a specific network will probably change how the IGP selects the best pathway for multiple networks on the other router. By running BGP, it is easier to manipulate individual networks for path selection, but all router administrators will need to have enough knowledge about BGP and its path selection process to troubleshoot routing problems across the AS.

The route that the inbound packets take to reach the AS is decided outside the AS (within the ISPs and other autonomous systems).

Full Routing Table from Each Provider

This topic examines receiving the full Internet routing table from each ISP and configuring BGP on at least the core or backbone routers for an AS. This topic discusses the benefits and limitations of this approach and explains that ISPs use a variation of this option by running BGP on every router in their AS.

Full Routes from All Providers

Cisco.com

- **Higher memory and CPU usage**
- **Reach all destinations by best path**
 - **Usually shortest AS path**
- **Can manually tune all pathways**

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-11

In the third design option of multihoming, all ISPs pass all routes to the AS, and IBGP is run on at least the core routers in this AS. The core routers need to be the equivalent of area 0 routers in an OSPF network or the backbone of a large internetwork.

To handle the full BGP routing table requires a high-end processor and at least 256 MB of RAM, which are usually found on Cisco 7200 or larger routers. The routers found at the distribution layer and access layer need to process the constant updates of BGP or handle the full Internet routing table.

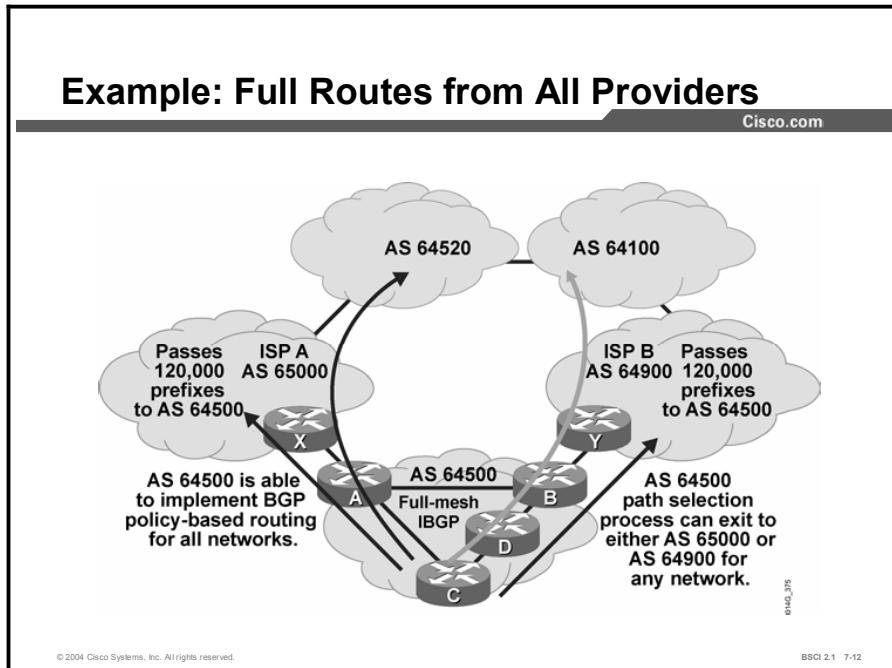
Usually, the distribution and access layer routers are in a stub or totally stubby area for OSPF and have a default route for all externally learned networks.

This configuration requires a lot of resources within the AS because you must process all the external routes. The AS sends all its routes to the ISPs, which process the routes and pass them to other autonomous systems.

The ISP that a specific router within the AS uses to reach the external networks is usually the shortest AS path; however, you can override this setting on any route.

The route that inbound packets take to reach the AS is decided outside the AS (within the ISPs and other autonomous systems); you can influence it by using the MED.

Example



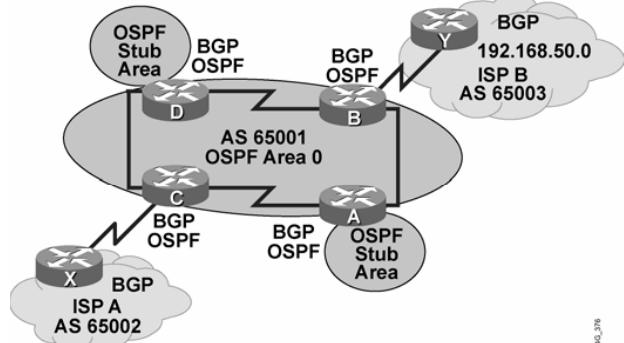
In this figure, AS 65000 and AS 64900 send all routes into AS 64500. The ISP that a specific router within AS 64500 uses to reach the external networks is usually the shortest AS path.

However, you can configure the routers in AS 64500 to influence the path to certain networks. For example, router A and router B can use a route map to set the local preference of certain routes to influence the outbound traffic from AS 64500.

Synchronization between the IGP and BGP needs to be turned off because no redistribution is being performed between the two routing protocols (BGP and the IGP), and thus the IGP will never have the BGP routes introduced into it.

Run BGP on Core Routers and Turn Off Synchronization

Cisco.com



- OSPF processes all local packets for the networks that are owned by AS 65001.
- BGP processes all packets moving across AS 65001 to other autonomous systems.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 - 7-13

In the figure, all routers in AS 65001 run both OSPF and BGP. OSPF processes all the local routing of packets between points in AS 65001. BGP processes the routing between local clients and the Internet and handles how traffic enters and leaves AS 65001. OSPF handles how traffic is routed between local clients and servers in AS 65001.

Problems on the Internet will not affect employees accessing corporate resources because OSPF and BGP are not communicating with each other. Each is doing its assigned job. This approach is known as SIN (“ships in the night”) routing because OSPF and BGP updates share the same bandwidth and routers but each is performing a different and unrelated function.

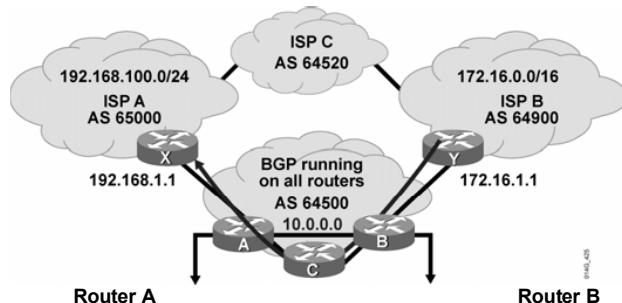
OSPF is handling traffic local to the AS, while BGP handles traffic between the AS and other autonomous systems. BGP, with its TCP flow control, is designed to process the constant changes that occur on the Internet.

Each router turns off BGP synchronization because full-mesh IBGP is being run and routes are not being redistributed from BGP into IGP.

ISPs usually run BGP on every router. For a non-ISP AS, BGP is configured on the core routers, or the area 0 routers if you are running OSPF. OSPF should be configured on all routers, and default routes should be sent into the other OSPF areas, which should be configured as OSPF stub or totally stubby areas.

Filter BGP Advertisements to ISPs

Cisco.com



```
router bgp 64500
network 10.0.0.0
neighbor 192.168.1.1 remote-as 65000
neighbor 192.168.1.1 distribute-list 7 out
(text omitted)
access-list 7 permit 10.0.0.0 0.255.255.255
```

```
router bgp 64500
network 10.0.0.0
neighbor 172.16.1.1 remote-as 64900
neighbor 172.16.1.1 distribute-list 7 out
(text omitted)
access-list 7 permit 10.0.0.0 0.255.255.255
```

Prevent a non-ISP (stub) AS from becoming a transit network by performing route advertisement filtering using access lists.

©2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-14

If a dual-homed customer, like AS 64500 in the figure, is passing the BGP routes that it has learned from one ISP out to the other ISP, then the customer AS can become a transit AS, which can cause the two ISPs to pass traffic through the customer AS. This situation is very undesirable for the dual-homed customer. The dual-homed customer just wants to have a redundant Internet connection but does not want to act as a transit AS between the two ISPs.

As the figure shows, the purpose of running BGP on all internal routers is to allow the routers in AS 64500 to manipulate the flow of traffic to and from AS 64500. In this case, AS 64500 can become a transit AS, which allows for packets to flow across AS 64500 from one ISP to another ISP.

In the figure, router B learns about network 172.16.0.0/16 from router Y in AS 64900 (ISP B). Router B passes the 172.16.0.0/16 network advertisement through IBGP to router A. Router A then passes the 172.16.0.0/16 network advertisement through EBGP to router X in AS 65000 (ISP A). The routers in AS 65000 now have two pathways to reach AS 64900, one pathway through ISP C (AS 64520) and the other through AS 64500, the dual-homed customer that is not an ISP.

You do not want to use the bandwidth of AS 64500 as a pathway between the ISPs, so you should enable the routers in AS 64500 to allow only the networks that they own to be advertised to their ISPs.

The configuration examples in the figure use a distribute list linked to a specific BGP neighbor to determine which networks are announced to that neighbor. AS 64500 owns network 10.0.0.0/8 and announces only this network to both EBGP neighbors and denies all other networks. The distribution list filter is applied to only the EBGP neighbors so that the information that is learned from the other autonomous systems still propagates to other BGP routers in AS 64500. The edge routers do not forward any networks external to AS 64500 to other autonomous systems.

Because other autonomous systems do not learn about networks and autonomous systems behind AS 64500, those autonomous systems cannot use AS 64500 as a transit AS to reach other networks.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **BGP multihoming increases the reliability of the connection to the Internet as well as the performance of the connection.**
- **The three design options available to implement multihoming are the following:**
 - Receiving a default route from each provider and passing it to internal routers can be beneficial, but for administrators there are important considerations.
 - Receiving a partial routing table from each provider can be beneficial, but it also has limitations.
 - Receiving the full Internet routing table from each provider and configuring BGP on internal routers can be beneficial.

© 2004 Cisco Systems, Inc. All rights reserved.

BSCI 2.1 7-15

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 7-4: BGP Path Manipulation Using the MED and Local Preference with Route Maps

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 three common ways to perform multihoming? (Choose three.)
- A) Each ISP passes only a default route to the AS.
 - B) Each ISP passes a default route and selected specific routes to the AS.
 - C) Each ISP passes selected specific routes but no default route to the AS.
 - D) Each ISP passes all routes to the AS.
- Q2) Which two conditions are true for accepting a default route from all providers? (Choose two.)
- A) The ISP always decides inbound paths to the customer AS.
 - B) The default route should not be passed into the IGP. Instead, static default routes should be configured on all routers that are not running BGP.
 - C) Path selection to reach specific networks is easy to manipulate.
 - D) There is low CPU and memory utilization as compared to the other choices.
- Q3) Of the following cases, which two demonstrate the benefits and concerns of receiving a partial routing table from each provider and redistributing it into the local routing protocol? (Choose two.)
- A) This method can be used when not all of the routers in an autonomous system run BGP; however, you must perform path manipulation across the autonomous system.
 - B) Redistributing a partial BGP forwarding table into the IGP is possible; however, you should use caution and good filtering.
 - C) Redistributing the full routing table from BGP to an IGP is commonly used as long as you perform some route filtering.
 - D) Redistribution between exterior gateway protocols (EGP) and internal gateway protocols (OSPF and RIP) is not possible.
- Q4) What are the three characteristics of receiving the full BGP forwarding table from each ISP? (Choose three.)
- A) ability to leave synchronization on and redistribute the BGP routes into the local routing protocol
 - B) higher memory and CPU utilization than when an AS receives a default route or partial routing table from each ISP
 - C) ability to reach all destinations by a best-path selection instead of a default path selection
 - D) ability to influence not only how packets exit the AS but also how they enter the AS

Quiz Answer Key

Q1) A, B, D

Relates to: Design Choices with Multihoming for BGP

Q2) A, D

Relates to: Default Route from Each Provider

Q3) A, B

Relates to: Partial Routing Table from Each Provider

Q4) B, C, D

Relates to: Full Routing Table from Each Provider

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:

- Quiz 7-1: BGP Overview
- Quiz 7-2: BGP Concepts and Terminology
- Quiz 7-3: Basic BGP Operations
- Quiz 7-4: BGP Route Summarization
- Quiz 7-5: BGP Path Selection Process
- Quiz 7-6: Basic BGP Path Manipulation Using Route Maps
- Quiz 7-7: Design Options for Multihoming

Quiz 7-1: BGP Overview

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

Objectives

This quiz tests your knowledge of how to:

- Describe the characteristics of BGP
- List BGP message types

Quiz

Answer these questions:

- Q1) Which two characteristics are true for BGP? (Choose two.)
- A) supports VLSM
 - B) supports CIDR
 - C) is an IGP
 - D) is not used for routing between autonomous systems
- Q2) Which two statements are true for BGP route advertisements and path selection? (Choose two.)
- A) BGP selects the best path based on speed.
 - B) BGP metrics are called attributes.
 - C) BGP advertises pathways.
 - D) BGP pathways are not loop-free.
- Q3) Which protocol does BGP use?
- A) UDP port 520
 - B) TCP port 179
 - C) IP protocol number 88
 - D) IP protocol number 89
- Q4) Which component does a BGP update contain?
- A) multiple pathways and multiple networks
 - B) a single pathway and multiple networks
 - C) a single pathway and a single network
 - D) multiple pathways and a single network
- Q5) Which BGP message is sent when an error condition is detected?
- A) BGP update message
 - B) BGP keepalive message
 - C) BGP open message
 - D) BGP notification message

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-2: BGP Concepts and Terminology

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

Objectives

This quiz tests your knowledge of how to:

- Identify the proper terms for describing various BGP routers and their relationships
- Describe the requirements for establishing an external BGP neighbor relationship
- Describe the requirements for establishing an internal BGP neighbor relationship
- State why IBGP route propagation requires fully meshed adjacencies

Quiz

Q1) Test your understanding of BGP terminology by matching terms with statements. Write the letter of the statement in front of the term that the statement describes. A statement can describe more than one term. Each term can fit multiple statements but choose only the statement that best describes the term.

Term

- 1. IBGP neighbors
- 2. BGP speakers
- 3. BGP neighbors
- 4. EBGP neighbors
- 5. BGP routers
- 6. BGP peers

Statement

- A) Routers that are advertising BGP routing information.
- B) A set of BGP routers that are explicitly configured to exchange BGP information. They will establish a TCP connection with each other.
- C) A set of BGP peers that, by default, can be multiple routers away, but both neighbors are in the same AS.
- D) A set of BGP peers that, by default, must be directly connected, and both neighbors must be in different autonomous systems.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-3: Basic BGP Operations

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

Objectives

This quiz tests your knowledge of how to:

- Describe basic BGP operations
- Identify BGP neighbor states
- Use BGP **show**, **debug**, and **clear** commands

Quiz

Answer these questions:

- Q1) Which command is used to administratively disable a BGP neighbor?
- A) **neighbor {ip-address | peer-group-name} shutdown**
 - B) **neighbor {ip-address | peer-group-name} update-source interface-type interface-number**
 - C) **neighbor {ip-address | peer-group-name} remote-as autonomous-system**
 - D) **neighbor {ip-address | peer-group-name} next-hop-self**
- Q2) Which command sets the next-hop address to be the source IP address of the update when advertising to a BGP neighbor?
- A) **neighbor {ip-address | peer-group-name} shutdown**
 - B) **neighbor {ip-address | peer-group-name} update-source interface-type interface-number**
 - C) **neighbor {ip-address | peer-group-name} remote-as autonomous-system**
 - D) **neighbor {ip-address | peer-group-name} next-hop-self**
- Q3) Which **clear ip bgp** command is the least intrusive for resetting a BGP session after changing outbound policy for neighbor 200.100.50.1?
- A) **clear ip bgp ***
 - B) **clear ip bgp 200.100.50.1 soft out**
 - C) **clear ip bgp 200.100.50.1**
 - D) **clear ip bgp 200.100.50.1 soft in**
- Q4) The **network** command that is used in the router BGP process identifies the interfaces out of which to advertise BGP updates.
- A) true
 - B) false
- Q5) BGP automatically peers with any other BGP neighbor.
- A) true
 - B) false

- Q6) Which BGP neighbor state is the proper state for normal BGP neighbor operations?
- A) active
 - B) open confirm
 - C) idle
 - D) established
- Q7) Which command resets the TCP session between a router and only its neighbor, 192.168.200.1?
- A) **clear ip bgp 192.168.200.1**
 - B) **clear ip bgp ***
 - C) **clear ip BGP 192.168.200.1 soft in**
 - D) **clear ip bgp 192.168.200.1 soft out**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-4: BGP Route Summarization

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

Objectives

This quiz tests your knowledge of how to:

- Explain how BGP4 is related to CIDR
- Explain how BGP implements route summarization with the **network** command
- Describe how BGP implements route summarization with the **aggregate-address** command

Quiz

Answer these questions:

- Q1) Consider the following configuration and routing table for router A. Assume default settings for all else.

```
router bgp 65001
neighbor 192.168.1.1 remote-as 65002
network 172.16.0.0
network 192.168.0.0 mask 255.255.0.0
show ip route
C    192.168..2.0/24 is directly connected, Ethernet 0/0
O    IA      192.168.0.0/16 [110/990] via 192.168.2.1,
00:00:03, Ethernet 0/0
172.16.0.0/24 is subnetted, 2 subnets
O      172.16.1.0/24 [110/660] via 10.2.1.1, 00:00:03, Ethernet
0/0
O      172.16.2.0/24 [110/770] via 10.2.1.1, 00:00:03, Ethernet
0/0
```

What networks does BGP announce?

- A) Router A announces 172.16.1.0/24, 172.16.2.0/24, 192.168.2.0/24, and 192.168.0.0/16.
- B) Router A announces 172.16.1.0/24, 172.16.2.0/24, and 192.168.2.0/24.
- C) Router A announces 172.16.0.0/16 and 192.168.0.0/16.
- D) Router A announces 172.16.0.0/16 and 192.168.2.0/24.

Q2) Consider this configuration:

```
router bgp 64200
neighbor 172.16.1.1 remote-as 64400
network 192.168.80.0
network 192.168.81.0
network 192.168.82.0
network 192.168.83.0
network 192.168.80.0 mask 255.255.252.0
ip route 192.168.80.0 255.255.252.0 null0
```

What does the router announce to neighbor 172.16.1.1?

- A) 192.168.80.0/22
- B) 192.168.80.0/24, 192.168.81.0/24, 192.168.82.0/24, 192.168.83.0/24, and 192.168.80.0/22
- C) 192.168.80.0/24, 192.168.81.0/24, 192.168.82.0/24, and 192.168.83.0/24
- D) The router does not announce anything because the **mask** option is not specified for the /24 networks and autosummary is on by default. Therefore, the /22 network is not announced.

Q3) Which command performs these tasks?

- announces the summarized block of 192.168.100.0/22
 - announces the more specific networks which are part of that block
 - installs a BGP route to null 0 for this summarization in the routing table
- A) **aggregate-address 192.168.100.0 255.255.252.0**
 - B) **network 192.168.100.0 mask 255.255.252.0**
 - C) **aggregate-address 192.168.100.0 255.255.252.0 summary-only**
 - D) **aggregate-address 192.168.100.0 255.255.252.0 as-set**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-5: BGP Path Selection Process

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

Objectives

This quiz tests your knowledge of how to:

- List the characteristics of BGP attributes
- Describe the AS path attribute
- Identify the characteristics of the next-hop attribute and its behavior
- Describe the origin attribute
- Describe the local preference attribute and its usage
- Describe the MED attribute and its usage
- Describe the weight attribute and its usage
- Describe BGP path selection criteria
- Explain the BGP path selection decision process

Quiz

Answer these questions:

- Q1) Which characteristic best describes the attribute? Match the BGP attributes to their characteristics by writing the letter of the characteristic that describes the attribute in front of the attribute. The same characteristic can be used for more than one attribute, but each attribute will have only one characteristic. Each correct answer is worth 6 points.

Attribute

- _____ 1. AS path
- _____ 2. next-hop
- _____ 3. local preference
- _____ 4. MED
- _____ 5. origin
- _____ 6. weight
- _____ 7. community

Characteristics

- A) well-known mandatory
- B) well-known discretionary
- C) optional transitive
- D) optional nontransitive
- E) proprietary to Cisco-

- Q2) Place the BGP selection criteria in order from the first step to the last step evaluated to select the BGP pathway that is submitted to the IP routing table. The first and last criteria (A and J) have been identified for you. Order the remaining criteria by placing a number in the space that is provided. Each correct answer is worth 7 points.
- A) _____ Prefer the path with the lowest neighbor BGP router ID
 - B) _____ Prefer lowest MED (from other autonomous system)
 - C) _____ Prefer shortest AS path
 - D) _____ Prefer oldest route for EBGP paths
 - E) _____ Prefer lowest origin code (IGP < EGP < incomplete)
 - F) _____ Prefer highest weight (local to router)
 - G) _____ Prefer the path through the closest IGP neighbor
 - H) _____ Prefer highest local preference (global within AS)
 - I) _____ Prefer route that was originated by the local router
 - J) _____ Prefer EBGP path over IBGP path

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-6: Basic BGP Path Manipulation Using Route Maps

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

Objectives

This quiz tests your knowledge of how to:

- Use route maps to set local preference
- Use route maps to set the MED

Quiz

Answer these questions:

Q1) When you use route maps to set local preference, which two statements are true?
(Choose two.)

- A) The higher value for local preference is preferred.
- B) Local preference is used only between EBGP neighbors.
- C) The lower value for local preference is preferred.
- D) Local preference is used only between IBGP neighbors.

Q2) Which two statements are true when you are using route maps to set the MED?
(Choose two.)

- A) The higher value for the MED is preferred.
- B) The MED is used between EBGP neighbors only.
- C) The lower value for the MED is preferred.
- D) The MED is used between IBGP neighbors only.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Quiz 7-7: Design Options for Multihoming

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

Objectives

This quiz tests your knowledge of how to:

- List three design options that are used to manipulate path selection when you are multihoming in BGP
- Describe the benefits of receiving a default route from each provider and passing it to internal routers
- Identify the benefits of receiving a partial routing table from each provider
- Identify the benefits of receiving the full Internet routing table from each provider and configuring BGP on internal routers

Quiz

Answer these questions:

- Q1) Which design option is best for an ISP connecting to at least two other ISPs?
- A) full Internet routing table from each ISP
 - B) default route from each ISP
 - C) full Internet routing table and default route for each ISP
 - D) partial Internet routing table from each ISP
- Q2) Which multihoming design option is best for a company that wants to minimize overhead and is not concerned about path selection to reach IP networks on the Internet?
- A) full Internet routing table from each ISP
 - B) default route from each ISP
 - C) full Internet routing table and default route for each ISP
 - D) partial Internet routing table from each ISP
- Q3) Which design option is best for a company that needs to make path selection for a limited number of known external autonomous systems and wants to redistribute BGP into its internal routing protocol of OSPF?
- A) full Internet routing table from each ISP
 - B) default route from each ISP
 - C) full Internet routing table and default route for each ISP
 - D) partial Internet routing table from each ISP

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Lesson Assessment Answer Key

Quiz 7-1: BGP Overview

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

Quiz 7-2: BGP Concepts and Terminology

- Q1) 1-C, 2-A, 3-B, 4-D, 5-A, 6-B

Quiz 7-3: Basic BGP Operations

- Q1) A
- Q2) D
- Q3) B
- Q4) B
- Q5) B
- Q6) D
- Q7) A

Quiz 7-4: BGP Route Summarization

- Q1) C
- Q2) B
- Q3) A

Quiz 7-5: BGP Path Selection Process

- Q1) 1-A, 2-A, 3-B, 4-D, 5-A, 6-E, 7-C
- Q2) A-10, B-6, C-4, D-9, E-5, F-1, G-8, H-2, I-3, J-7

Quiz 7-6: Basic BGP Path Manipulation Using Route Maps

- Q1) A, D
- Q2) B, C

Quiz 7-7: Design Options for Multihoming

- Q1) C
- Q2) B
- Q3) D

Lab Guide

Overview

Use this guide 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: Basic Connectivity
- Lab Exercise 1-2: NAT Using Access Lists and Route Maps
- Lab Exercise 2-1: Migrating to a Classless Routing Protocol
- Lab Exercise 3-1: Configuring and Tuning EIGRP
- Lab Exercise 4-1: Configuring and Examining OSPF in a Single Area
- Lab Exercise 4-2: Configuring OSPF for Multiple Areas and Frame Relay NBMA
- Lab Exercise 4-3: Configuring OSPF for Multiple Areas and Frame Relay Point-to-Multipoint and Point-to-Point
- Lab Exercise 4-4: Understanding the OSPF Database and Tuning OSPF
- Lab Exercise 4-5: Configuring OSPF Virtual Links (Optional)
- Lab Exercise 5-1: Configuring Integrated IS-IS in Multiple Areas
- Lab Exercise 6-1: Configuring Basic Redistribution
- Lab Exercise 6-2: Tuning Basic Redistribution with Cisco IOS Tools
- Lab Exercise 6-3: Configuring Policy-Based Routing (Optional)
- Lab Exercise 7-1: Configuring EBGP for Two Neighbors
- Lab Exercise 7-2: Configuring Fully Meshed IBGP
- Lab Exercise 7-3: Configuring BGP Route Summarization and Examining the BGP Path Selection Process
- Lab Exercise 7-4: BGP Path Manipulation Using the MED and Local Preference with Route Maps

Lab Exercise 1-1: Basic Connectivity

Complete this lab exercise to practice what you learned in the related lesson.

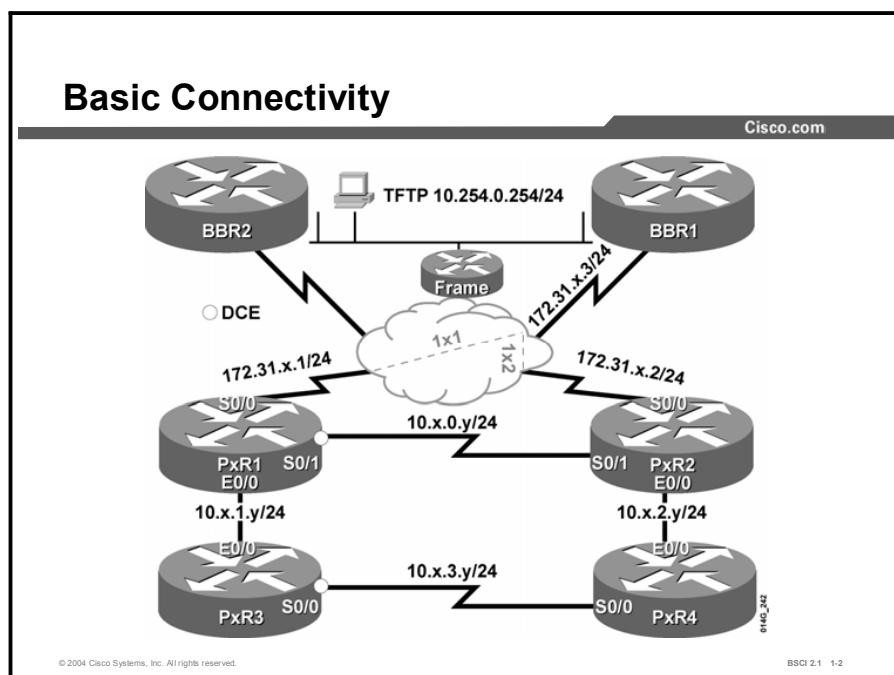
Exercise Objective

In this exercise, you will connect to the edge routers (PxR1 and PxR2) and download a configuration file in order to set up an edge router. After completing this exercise, you will be able to meet these objectives:

- Connect to the TFTP server in the core from the PxR1 and PxR2 routers
- Download a configuration file and complete the setup of your edge routers (PxR1 and PxR2)

Visual Objective

The figure illustrates what you will accomplish in this exercise.



The figure shows the complete topology of the lab equipment. In this exercise you will connect the edge routers (PxR1 and PxR2) to Backbone Router 1 (BBR1) over the Frame Relay network and download a file from the TFTP server.

Note	Throughout the exercise the pod number is referred to with x and the router number with y. Substitute the appropriate number as needed.
-------------	---

Required Resources

These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4 (where x is the pod number) and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	
REMOTE IP	
REMOTE Port	
REMOTE Username and Password	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
<code>(config-if)#encapsulation frame-relay</code>	Enables Frame Relay encapsulation.
<code>(config-if)#frame-relay map ip 172.31.x.3 1x1 broadcast</code>	Maps a next-hop IP address to a permanent virtual circuit (PVC).
<code>(config-if)#ip address 172.31.x.1 255.255.255.0</code>	Assigns an IP address.
<code>(config)#ip route 10.0.0.0 255.0.0.0 172.31.x.3</code>	Creates a static route.
<code>(config-if)#no shutdown</code>	Brings up an interface.

Job Aids

There are no job aids for this lab exercise.

Task 1: Setting Up the Edge Router

In this task, you will use a Telnet or terminal utility to establish a connection to the lab equipment for this course. For the purpose of this exercise procedure, substitute your pod number for *x* and your router number for *y*.

Exercise Procedure

Complete these steps:

- Step 1** Connect to your assigned edge routers (PxR1 and PxR2). Your router does not have a configuration on it. If your router has a configuration, delete the configuration using the **erase start** command, and then use the **reload** command to reboot.

Note You will need to apply some minimal addressing and routing information to reach the TFTP server.

- Step 2** Configure the serial s0/0 interface for Frame Relay by turning on Frame Relay encapsulation.

- Step 3** Assign an IP address to your serial 0/0 interface. Your IP address is 172.31.x.y/24, where *x* is your pod number and *y* is your router number.

- Step 4** **Inverse arp** has been turned off in your Frame Relay network. Manually map a Data Link Connection Identifier (DLCI) to BBR1 (172.31.x.3). The DLCI number will be in the form 1xy where *x* is your pod number and *y* is your router number. For instance, P2R1 will use DLCI 121.

Note	Remember to specify the broadcast keyword so that the mapping supports broadcasts and multicasts such as routing protocol traffic.
-------------	---

Step 5 No shut the interface and exit configuration mode.

Step 6 Verify successful connectivity from your PxR1 and PxR2 router to the core BBR1 router (172.31.x.3) using the **ping** command.

Step 7 The goal is to download a file from the TFTP server (10.254.0.254), which is connected to BBR1. However, a look at your PxR1 and PxR2 routing table reveals that there is not a route to reach the TFTP server. Your display should resemble the following:

```
router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is not set
    172.31.0.0/24 is subnetted, 1 subnets
      C      172.31.x.0 is directly connected, Serial0/0
```

Step 8 Add a static route to 10.0.0.0/8 through BBR1 (172.31.x.3) to provide a path to the TFTP server. Your **show ip route** display should resemble the following:

```
router#show ip route
00:30:05: %SYS-5-CONFIG_I: Configured from console by console
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B- BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
          i - IS-IS, L1- IS-IS level-1, L2- IS-IS level-2, ia - IS-
IS inter area
          * - candidate default, U - per-user static route, o - ODR
          P - periodic downloaded static route
Gateway of last resort is not set
```

```
    172.31.0.0/24 is subnetted, 1 subnets
C      172.31.x.0 is directly connected, Serial0/0
S      10.0.0.0/8 [1/0] via 172.31.x.3
```

Step 9 Verify successful connectivity to the TFTP server (10.254.0.254) from your PxR1 and PxR2 routers using the **ping** command.

Step 10 Use TFTP on the edge router to obtain from the TFTP server a setup file named for your router: PxRy.txt (Pod 5 Router 2 will download P5R2.txt). Your display should resemble the following:

```
router#copy tftp run
Address or name of remote host []? 10.254.0.254
Source filename []? PxRy.txt
Destination filename [running-config]?
```

Note The setup file includes **no ip classless** to force your router to behave classfully. In addition, it includes all required IP addresses and enables all required interfaces. Remember that files copied to running-config are merged, so this file will complement what is already in your running-config.

Step 11 An example of a setup file is shown below:

```
host P3R2
no ip domain-lookup
no ip classless
enable secret cisco
line con 0
logging synchronous
exec-timeout 30 0
line vty 0 4
no login
exit
int s0/0
no frame-relay inverse-arp
int s0/1
ip address 10.3.0.2 255.255.255.0
no shutdown

int e0/0
ip address 10.3.2.2 255.255.255.0
no shutdown
exit
```

Step 12 Save your configuration before proceeding.

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You can ping the core BBR1 router and the TFTP server from your PxR1 and PxR2 router.
- You have downloaded the configuration file for your assigned router from the TFTP server.

Lab Exercise 1-2: NAT Using Access Lists and Route Maps

Complete this lab exercise to practice what you learned in the related lesson.

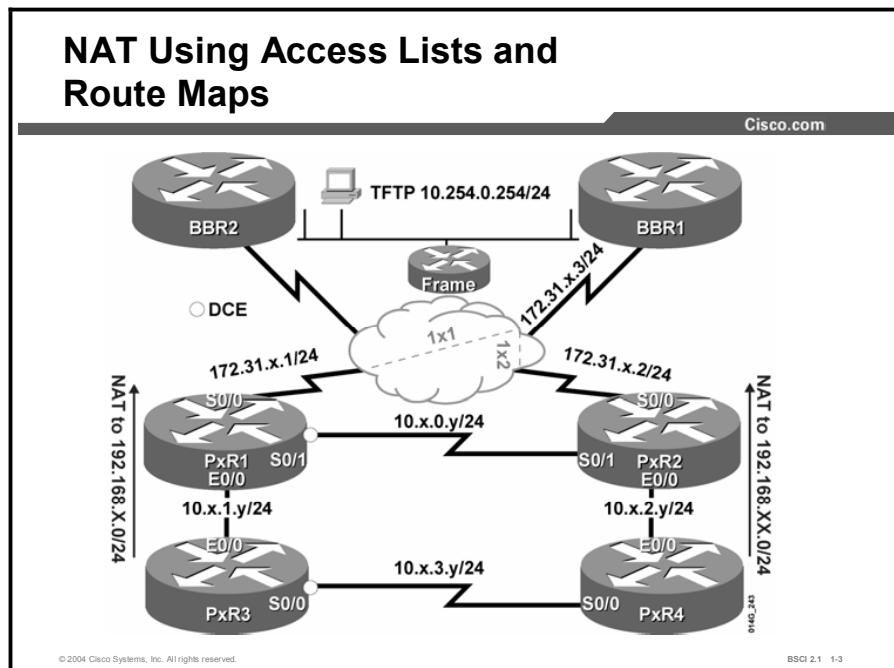
Exercise Objective

In this exercise, you will use NAT to allow your internal routers (PxR3 and PxR4) to download a configuration file from the TFTP server. After completing this exercise, you will be able to meet these objectives:

- List the uses and limits of access-list-based NAT
- Demonstrate the usefulness of NAT with route maps by implementing separate concurrent translations
- Connect the internal router to the TFTP server or the opposite edge router using appropriate translation
- Download a configuration file for the internal routers

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Note Throughout the exercise the pod number is referred to with x and the router number with y. Substitute the appropriate number as needed.

Required Resources

These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4 and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
<code>(config)#access-list 100 permit ip 10.1.x.0 0.0.0.255 10.254.0.0 0.0.0.255</code>	Specifies traffic that should be translated.
<code>#clear ip nat translation *</code>	Removes all address translations from the NAT table.
<code>#debug ip nat detail</code>	Witnesses translation entries being created.
<code>(config-if)#ip nat inside</code>	Identifies an internal private interface and address.
<code>(config)#ip nat inside source list 100 pool BBR</code>	Translates inside addresses that match this access list into this pool.
<code>(config)#ip nat inside source route-map TO_POOL pool POD</code>	Specifies a route map to be used for NAT.
<code>(config-if)#ip nat outside</code>	Identifies an external public interface and address.
<code>(config)#ip nat pool BBR 192.168.x.1 192.168.x.254 netmask 255.255.255.0</code>	Creates a named pool of real addresses for use by NAT.
<code>(config)#ip nat pool BBR 192.168.x.1 192.168.x.254 prefix-length 24</code>	Creates a named pool of real addresses for use by NAT—the subnet mask is specified by the number of ones (the prefix length).
<code>(config)#route-map TO_BBR permit 10 match ip address 100</code>	Creates a route map to match the source address.
<code>#show ip nat translations</code>	Views the translation table.

Job Aids

There are no job aids for this lab exercise.

Task 1: Connecting the Internal Router to the Edge Router

In this task, you will use a Telnet or terminal utility to establish a connection to the lab equipment for this course. For the purpose of this exercise procedure, substitute your pod number for “x” and your router number for “y.”

Exercise Procedure

Complete these steps:

- Step 1** The internal router should not have a configuration. If a configuration is present, you should use the **erase start** and **reload** commands to clear the router.
- Step 2** Connect to your internal routers (PxR3 and PxR4). Supply an IP address to the Ethernet interface and enable the interface. The Ethernet address of PxR3 should be 10.x.1.3/24, and the Ethernet address of PxR4 should be 10.x.2.4/24.

- Step 3** PxR1 has an Ethernet address of 10.x.1.1, and PxR2 is 10.x.2.2. Verify connectivity to the Ethernet-attached edge router from each internal router. Your display should resemble the following:

```
router#ping 10.2.1.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.2.1.1, timeout is 2  
seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max =  
1/1/4 ms
```

Task 2: Setting Up Access-List-Based NAT

In this task, you will configure one-to-one NAT using an access list on the edge router (PxR1 or PxR2). The access list translates the internal router Ethernet address to the TFTP server using either 192.168.x.0/24 or 192.168.xx.0/24. BBR1 has static routes for 192.168.x.0/24 and 192.168.xx.0/24. It does not have any remote routes for the pod 10.x.0.0 addresses, but only its local TFTP server network 10.254.0.0.

Exercise Procedure

Complete these steps:

- Step 1** At the PxR1 and PxR2 routers, identify what sources will be translated by configuring an extended access list 100. Access list 100 should match traffic that is sourced from the network on the Ethernet interface of your edge router, destined for the network of the TFTP server.
- For instance, PxR1 should match traffic sourced from 10.x.1.0/24, and PxR2 should match sourced traffic from 10.x.2.0/24. The access list must additionally match packets with a destination of 10.254.0.0/24.
- Step 2** At the PxR1 and PxR2 routers, create a pool of addresses that is named “BBR” for use by NAT, using the **ip nat pool** command. PxR1 should use the address range of 192.168.x.0/24, and PxR2 should use 192.168.xx.0/24. For instance, P5R1 would use 192.168.5.1-254, and P5R2 would use 192.168.55.1-254.
- Step 3** At the PxR1 and PxR2 routers, use the **ip nat inside source list** command to specify that packets that match access list 100 should have source addresses translated into the BBR pool.
- Step 4** At the PxR1 and PxR2 routers, define which interfaces are inside or outside the NAT translation. Because the traffic to be translated will be coming from the Ethernet interface, the Ethernet interface will be the inside NAT interface. Translated traffic will leave via the Serial0/0 interface, so the Serial0/0 interface will be the outside interface for NAT.
- Step 5** At the PxR3 and PxR4 routers, configure a default route pointing to the attached edge router e0/0 interface. This configuration allows the internal router to reach the core network.

- Step 6** From the PxR3 and PxR4 routers, verify connectivity to the TFTP server (10.254.0.254) using the **ping** command.

Caution You will not be able to reach the TFTP server if the NAT translation is not done correctly.

- Step 7** View the NAT translation table on the edge router (PxR1 and PxR2). Your display should resemble the following:

```
P3R2#sh ip nat trans
  Pro Inside global      Inside local      Outside local
  Outside global
  --- 192.168.33.1      10.3.2.4          ---
  --
P3R2#
```

Task 3: Translating to the Other Edge Router

In this task, you will need to translate traffic from the odd half of the pod (PxR1 and PxR3) to the even half (PxR2 and PxR4) and vice versa. Because you are not running a routing protocol, you will translate the interior addresses to addresses that would be appropriate on the serial link between PxR1 and PxR2.

Exercise Procedure

Complete these steps:

- Step 1** At the PxR1 and PxR2 routers, identify what sources will be translated by configuring an extended access list 101. Access list 101 should match traffic that is sourced from the network on the Ethernet interface of your edge router, bound to any destination.

For instance, PxR1 should match traffic from 10.x.1.0/24, and PxR2 should match traffic from 10.x.2.0/24. The access list must additionally match packets with a destination to any network.

- Step 2** At the PxR1 and PxR2 routers, create a pool of addresses that is named “POD” for use by NAT. PxR1 should use 10.x.0.64-95, and PxR2 should use 10.x.0.96-127.

- Step 3** At the PxR1 and PxR2 routers, specify that packets that match access list 101 should have source addresses translated into the POD pool.

- Step 4** At the PxR1 and PxR2 routers, put **ip nat out** on the s0/1 interface of each edge router so that traffic from the respective internal routers is translated.

- Step 5** This step involves troubleshooting: From one internal router, ping the Serial 0/1 interface of the nonconnected edge router (for instance, from PxR3 ping the Serial 0/1 address of PxR2). The following display indicates that pinging the opposite edge router is unsuccessful. Why is the ping unsuccessful?

```
P2R3#ping 10.2.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.2.0.2, timeout is 2  
seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

- Step 6** Look at the IP translation table of the edge routers. It has already translated this source address, and it does not recognize that this address is a separate conversation. It will not retranslate the traffic for the new destination. A way to recognize differing conversations is required. Your display should resemble the following:

```
P2r1#sh ip nat trans
```

Pro	Inside global	Inside local	Outside local
Outside global			
---	192.168.2.1	10.2.1.3	---

- Step 7** From the nonconnected edge router, use **debug ip icmp** and **debug ip packet** commands while the pings are still active. The output is reproduced below. The debug messages reveal why the ping from PxR3 was unsuccessful.

```
P2r2#debug ip icmp
```

```
ICMP packet debugging is on
```

```
P2r2#
```

```
2w1d: ICMP: echo reply sent, src 10.2.0.2, dst 192.168.2.1
```

```
2w1d: IP: s=10.2.0.2 (local), d=192.168.2.1, len 100,  
unreachable
```

- Step 8** Take a look at the routing table on your opposite edge router and try to find the route back to the destination address of the echo reply message. Your output should resemble the following example taken from Pod 2:

Note	Notice in the previous step that the destination address was 192.168.x.1.
-------------	---

```
P2R2#sh ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M -  
mobile, B - BGP
```

```
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF  
inter area
```

```
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external  
type 2
```

```
          E1 - OSPF external type 1, E2 - OSPF external type 2, E  
- EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -  
IS-IS inter area  
* - candidate default, U - per-user static route, o -  
ODR  
P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.31.0.0/24 is subnetted, 1 subnets  
C      172.31.2.0 is directly connected, Serial0/0  
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks  
C      10.2.0.0/24 is directly connected, Serial0/1  
C      10.2.1.0/24 is directly connected, Ethernet0/0  
S      10.0.0.0/8 [1/0] via 172.31.2.3
```

- Step 9** There is no route back to that address listed in the routing table. What does a router do when it does not find an appropriate address?

Task 4: Using a Route Map with NAT to Translate Internal Address

In this task, you will configure NAT using a route map to match traffic. You have seen that when NAT uses an access list without overloading addresses, the translation entry contains only local and global IP addresses. When a route map is used with NAT, the translation entry contains both the inside and outside (local and global) address entries and any TCP or UDP port information. This translation entry enables the router to recognize different conversations.

Exercise Procedure

Complete these steps:

- Step 1** Traffic needs to be translated based on destination. Traffic to the TFTP server and the core should still be translated to 192.168.x.0/24 or 192.168.xx.0/24, but traffic to the other edge router should be translated to an IP address in the 10.x.0.0 subnet.

This address will appear to be local to the serial 0/1 interface of the other edge and will have a path entered in the routing table (connected routes are automatically in the routing table).

To prevent confusion, PxR1 will use the range of 10.x.0.64-95/24, and PxR2 will use 10.x.0.96-127/24. Use a route map to conditionally translate traffic that is based on destination. Your display should resemble the following:

```
route-map TO_BBR permit 10  
  match ip address 100  
!  
route-map TO_POD permit 10  
  match ip address 101
```

- Step 2** Replace the old translation commands with a route-map-based translation. Your display should resemble the following:

```
P2R1(conf)#no ip nat inside source list 100 pool BBR
P2R1(conf)#no ip nat inside source list 101 pool POD
P2R1(conf)#ip nat inside source route-map TO_BBR pool BBR
P2R1(conf)#ip nat inside source route-map TO_POD pool POD
```

-
- Note** If the router reports "%Dynamic mapping in use, cannot remove", simply back out to privileged mode and enter **clear ip nat trans *** to remove all mappings.
-

- Step 3** Ping from one internal router to the opposite edge router and to the TFTP server to verify that the previous step was successful. Turn on **debug ip nat details** on the edge routers to see the translation. Your display should resemble the following:

From the internal router, ping the TFTP server:

```
P1R3#ping 10.254.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.254.0.254 , timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
36/36/40 ms
```

From the Edge router, enable **debug ip nat details**:

```
P1R1#
2w1d: NAT: s=10.1.1.3->192.168.1.1, d=10.254.0.254 [85]
2w1d: NAT*: s=10.254.0.254 , d=192.168.1.1->10.1.1.3 [85]
2w1d: NAT: s=10.1.1.3->192.168.1.1, d=10.254.0.254 [86]
2w1d: NAT*: s=10.254.0.254 , d=192.168.1.1->10.1.1.3 [86]
2w1d: NAT: s=10.1.1.3->192.168.1.1, d=10.254.0.254 [87]
2w1d: NAT*: s=10.254.0.254 , d=192.168.1.1->10.1.1.3 [87]
2w1d: NAT: s=10.1.1.3->192.168.1.1, d=10.254.0.254 [88]
2w1d: NAT*: s=10.254.0.254 , d=192.168.1.1->10.1.1.3 [88]
2w1d: NAT: s=10.1.1.3->192.168.1.1, d=10.254.0.254 [89]
2w1d: NAT*: s=10.254.0.254 , d=192.168.1.1->10.1.1.3 [89]
```

Again, from the internal router, ping the other edge router:

```
P1R3#ping 10.1.0.2
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 10.1.0.2, timeout is 2
seconds:
```

!!!!!

```
Success rate is 100 percent (5/5), round-trip min/avg/max =
20/20/24 ms
```

And again, from the edge router, enable **debug ip nat details**:

```
P1R1#  
2w1d: NAT: s=10.1.1.3->10.1.0.64, d=10.1.0.2 [90]  
2w1d: NAT*: s=10.1.0.2, d=10.1.0.64->10.1.1.3 [90]  
2w1d: NAT: s=10.1.1.3->10.1.0.64, d=10.1.0.2 [91]  
2w1d: NAT*: s=10.1.0.2, d=10.1.0.64->10.1.1.3 [91]  
2w1d: NAT: s=10.1.1.3->10.1.0.64, d=10.1.0.2 [92]  
2w1d: NAT*: s=10.1.0.2, d=10.1.0.64->10.1.1.3 [92]  
2w1d: NAT: s=10.1.1.3->10.1.0.64, d=10.1.0.2 [93]  
2w1d: NAT*: s=10.1.0.2, d=10.1.0.64->10.1.1.3 [93]  
2w1d: NAT: s=10.1.1.3->10.1.0.64, d=10.1.0.2 [94]  
2w1d: NAT*: s=10.1.0.2, d=10.1.0.64->10.1.1.3 [94]
```

- Step 4** View **show ip nat translations** on each edge router. Your display should resemble the following:

Note	Notice that the table is completely developed. A conditional translation has been made, and there is much more debugging information available within this table.
-------------	---

```
P1R1#show ip nat translations  
Pro Inside global      Inside local      Outside local  
Outside global  
icmp 192.168.1.1:7159  10.1.1.3:7159    10.254.0.1:7159  
10.254.0.1:7159  
icmp 192.168.1.1:7160  10.1.1.3:7160    10.254.0.1:7160  
10.254.0.1:7160  
icmp 192.168.1.1:7161  10.1.1.3:7161    10.254.0.1:7161  
10.254.0.1:7161  
icmp 192.168.1.1:7162  10.1.1.3:7162    10.254.0.1:7162  
10.254.0.1:7162  
icmp 192.168.1.1:7163  10.1.1.3:7163    10.254.0.1:7163  
10.254.0.1:7163  
icmp 10.1.0.64:3335    10.1.1.3:3335    10.1.0.2:3335  
10.1.0.2:3335  
icmp 10.1.0.64:3336    10.1.1.3:3336    10.1.0.2:3336  
10.1.0.2:3336  
icmp 10.1.0.64:3337    10.1.1.3:3337    10.1.0.2:3337  
10.1.0.2:3337  
icmp 10.1.0.64:3338    10.1.1.3:3338    10.1.0.2:3338  
10.1.0.2:3338
```

```
icmp 10.1.0.64:3339      10.1.1.3:3339      10.1.0.2:3339  
10.1.0.2:3339
```

Task 5: Downloading a Configuration File

Now that NAT is properly configured and working, you can download a configuration for the internal routers.

Exercise Procedure

Complete these steps:

- Step 1** On the internal routers (PxR3 and PxR4), use TFTP to download the setup file named PxRy.txt from the TFTP server to the running-config. The following display is for an example file (for P3R4):

```
host P3R4  
no ip domain-lookup  
no ip classless  
enable password cisco  
line console 0  
logging synchronous  
exec-timeout 30 0  
line vty 0 4  
no login  
exit  
int e 0/0  
ip address 10.3.2.4 255.255.255.0  
no shut  
int s0/0  
  
ip address 10.3.3.4 255.255.255.0  
no shut  
exit  
end
```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- Your interior router can ping the TFTP server using a translation to 192.168.x.0/24.
- Your interior router can ping the opposite edge router using a translation to 10.x.0.0/24.
- You have demonstrated the limitations of access-list-based NAT, and overcome those limitations by configuring NAT using a route map.
- You have connected to the TFTP server, through a NAT, and downloaded a configuration file.

Lab Exercise 2-1: Migrating to a Classless Routing Protocol

Complete this lab exercise to practice what you learned in the related lesson.

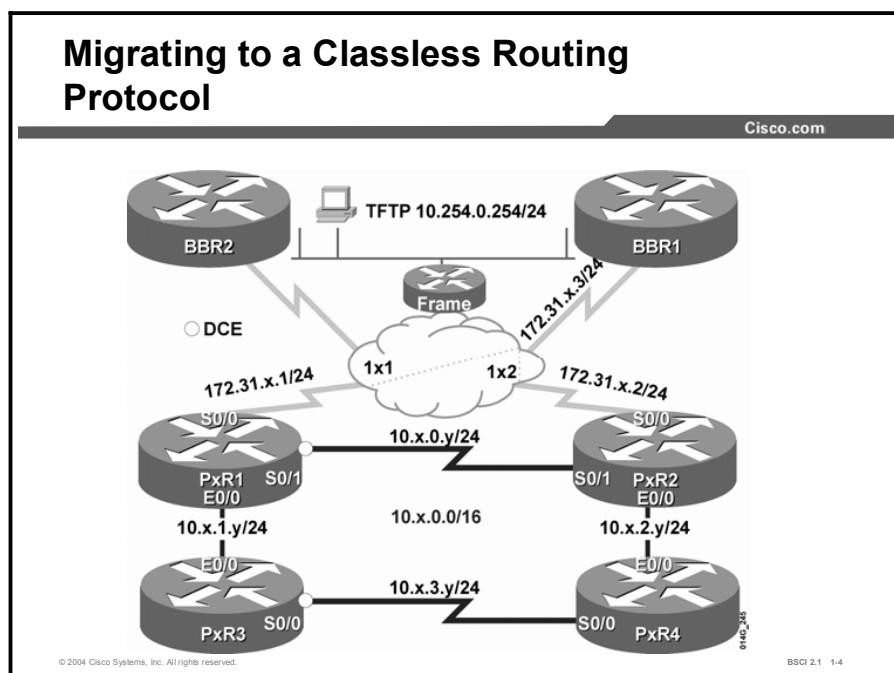
Exercise Objective

In this exercise, you will set up RIPv2. After completing this exercise, you will be able to meet these objectives:

- Connect to other devices in the network and have full network visibility using RIPv2 as a routing protocol
- Recognize RIPv2 support for default routes, VLSM, and route summarization
- Determine how VLSM contributes to network efficiency

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled R1 through R4) that are connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled R1 through R4 and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 1/1 port on R1 and R2.

In Task 1, you will need a terminal or Telnet utility to establish a connection to the remote lab equipment for this course.

Command List

The commands used in this exercise are described in the table here.

Table 1: Commands

Command	Description
(config-router) #default-information originate	Advertises the default route through RIP.
(config) #ip classless	Instructs the router to behave classlessly.
(config)#ip route 0.0.0.0 0.0.0.0 172.31.x.3	Creates a static default route.
(config-if)#ip summary-address rip 10.x.0.0 255.255.0.0	Advertises an arbitrary summarization.
(config-router) #network 172.31.0.0	Specifies a classful network that RIP should run within.
(config-router) #no auto-summary	Does not automatically summarize routes at classful boundaries.
(config)#router rip	Turns on RIP.
(config-router) #version 1	Runs RIPv1.
(config-router) #version 2	Runs RIPv2.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

In this task, you will establish a connection to the remote lab equipment for this course.

Exercise Procedure

Complete these steps:

- Step 1** The work on Network Address Translation (NAT) is complete and all access lists, route maps, NAT statements, and static routes should be manually removed from the routers.

Another way to do this is to copy the configuration file from the TFTP server (PxRy.txt) into **startup-config** and reload each router.

-
- Note** **IMPORTANT:** You must enable IP classless routing on the internal router before attempting to download the configuration file. Copy the configuration for the internal router before you reload the edge router.
-

If access to the TFTP server is not available, you should erase the startup-configuration and reload. Type in the commands below for the edge routers:

```
host PxRy
no ip domain-lookup
no ip classless
enable password cisco
line con 0
logging synchronous
exec-timeout 30 0
line vty 0 4
no login
exit
int s0/0
encap frame
frame map ip 172.31.x.3 1x1 broadcast
ip add 172.31.x.y 255.255.255.0
no frame-relay inverse-arp
no sh
int s0/1
ip address 10.x.0.y 255.255.255.0
clock rate 64000
no shutdown
int e0/0
ip address 10.x.1.y 255.255.255.0 (for routers PxR1 and PxR3)
or
```

```
ip address 10.x.2.y 255.255.255.0 (for routers PxR2 and PxR4)
no shutdown
end
```

For the internal routers, it is necessary only to remove the static routes. The configuration for the internal routers follows:

```
host PxRy
no ip domain-lookup
ip classless
enable password cisco
line con 0
logging synchronous
exec-timeout 30 0
line vty 0 4
no login
exit
int e 0/0
ip address 10.x.(y-2).y 255.255.255.0
no shut
int s0/0
ip address 10.x.3.y 255.255.255.0
clock rate 64000
no shut
end
```

Task 2: Exploring Classful Routing

In this task, you will explore classful routing.

Exercise Procedure

Complete these steps:

- Step 1** At the routers within your assigned pod, configure RIPv1 within the classful pod network (10.0.0.0) and class B 172.31.0.0 Frame Relay network on edge routers.
- Step 2** Explicitly specify RIPv1 using the **version 1** command. The default sends version 1 advertisements and receives versions 1 and 2. Setting the router to version 1 prevents confusion—the backbone router runs both versions.
- Step 3** Verify that your routers accept only version 1 advertisements using the command **show ip protocols**. The following example shows a router set to receive both types of advertisements. Your routers should list only version 1 under the “Recv” column.

```
P3R1#show ip protocol
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 23 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
```

```

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
      Interface          Send   Recv Triggered RIP Key-chain
      Ethernet0/0         1       1
      Serial0/0            1       1
      Serial0/1            1       1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.31.0.0
Routing Information Sources:
      Gateway        Distance     Last Update
      10.x.1.3        120          00:00:12
      172.31.x.3      120          00:00:09
Distance: (default is 120)

```

- Step 4** Test connectivity to the TFTP server (10.254.0.254 /24) from the interior router by using the ping utility. Why does the ping to the TFTP not work? Your display should resemble the following:

```

P3R4#ping 10.254.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.254.0.254, timeout is 2
seconds:
.....  

Success rate is 0 percent (0/5)

```

- Step 5** Classful routing behavior is to look for known routes within the connected classful network (10.0.0.0, in this case) and to not consider less specific routes. Classful routing protocols, such as RIPv1, do not exchange subnet mask information and are forced to either assume a constant mask throughout the classful network or to simply advertise the entire classful network.

Advertisements between the pod edge routers and BBR1 go across the 172.31.0.0 network. Therefore, all three routers summarize the subnets, and advertise network 10.0.0.0 to each other. Each router ignores this advertisement, because it already has a route to that network.

You can verify this behavior with the **debug ip rip** command. The interior router is therefore not able to reach the core because it does not have a route for this subnet in its routing table. Verify this situation by displaying the routing table on the internal router. Look for a route to the 10.254.0.0 network.

- Step 6** To allow the interior routers to reach the core, advertise a default route from the edge router through RIP. First, set up a static default route on the edge routers, and then advertise the route to your RIP neighbors using the **default-information originate** command under the router RIP configuration.
- Step 7** Look at the routing table on the interior router. Is there a path now? Remember that RIP is slow to converge. You may need to wait for up to a minute, even in this small network, before the default route appears on the interior router. To force convergence, you may issue the **clear ip route *** command. Your display should resemble the following:

```
P3R4#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
      * - candidate default, U - per-user static route, o -
ODR
      P - periodic downloaded static route
Gateway of last resort is 10.3.2.2 to network 0.0.0.0
      R    172.31.0.0/16 [120/1] via 10.3.2.2, 00:00:03, Ethernet0/0
          10.0.0.0/24 is subnetted, 2 subnets
      R    10.3.0.0 [120/1] via 10.3.2.2, 00:00:03, Ethernet0/0
      C    10.3.2.0 is directly connected, Ethernet0/0
      R*   0.0.0.0/0 [120/2] via 10.3.2.2, 00:00:03, Ethernet0/0
P3R4#
```

- Step 8** Once again, test connectivity from the interior router to the TFTP server using the ping utility. The ping to the TFTP server still did not work. Why not? Your display should resemble the following:

```
P3R4#ping 10.254.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.254.0.254, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
P3R4#
```

Task 3: Exploring Classless Forwarding

The ping to the TFTP server did not work because classful behavior, as discussed previously, is to look for known routes within the connected classful network (10.0.0.0, in this case) and to not consider less specific routes such as a default route. Given that classful behavior is the cause of the problem, explore classless behavior in the following steps.

Exercise Procedure

Complete these steps:

- Step 1** The TFTP server cannot be reached because the router has been instructed to route classfully with the command **no ip classless**. Classful routing behavior is to look for known routes within the connected classful network (10.0.0.0, in this case) and to not consider less specific routes.
- Step 2** Enable IP classless on each router to explore classless behavior.
- Step 3** Test connectivity from the interior router to the TFTP server.
- Step 4** Although you changed the router behavior, RIPv1 is still a classful routing protocol and is still autosummarizing across the Frame Relay link. The BBR1 router will not have a route back to the 10.x.1.0/24 or 10.x.2.0/24 subnets.

To remedy this situation, move to the classless version of RIP: RIPv2.

Additionally, turn off RIP automatic route summarization at the edge routers.

- Step 5** One more time, test connectivity from the interior router to the TFTP server. Your display should resemble the following:

```
P3R4#ping 10.254.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.254.0.254, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/34/36 ms
```

Task 4: Optimizing Classless Routes for Scalability

In this task you will optimize classless routes for scalability.

Exercise Procedure

Complete these steps:

- Step 1** From the interior router, use Telnet to connect to BBR1 (172.31.x.0). Notice that all of the networks of your pod are listed in the routing table of BBR1. Your display should resemble the following:

```
BBR1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is not set
    172.31.0.0/24 is subnetted, 2 subnets
      C        172.31.3.0 is directly connected, Serial0/0.3
      C        172.31.2.0 is directly connected, Serial0/0.2
    10.0.0.0/24 is subnetted, 5 subnets
      R        10.3.1.0 [120/1] via 172.31.3.1, 00:00:27, Serial0/0.3
      R        10.3.0.0 [120/1] via 172.31.3.2, 00:00:06, Serial0/0.3
                  [120/1] via 172.31.3.1, 00:00:27, Serial0/0.3
      R        10.3.3.0 [120/2] via 172.31.3.2, 00:00:06, Serial0/0.3
                  [120/2] via 172.31.3.1, 00:00:27, Serial0/0.3
      R        10.3.2.0 [120/1] via 172.31.3.2, 00:00:06, Serial0/0.3
      C        10.254.0.0 is directly connected, Ethernet0/0
      S        192.168.22.0/24 [1/0] via 172.31.2.2
      S        192.168.2.0/24 [1/0] via 172.31.2.1
      S        192.168.3.0/24 [1/0] via 172.31.3.1
      S        192.168.33.0/24 [1/0] via 172.31.3.2
BBR1#
```

- Step 2** As the size of the network grows, large routing tables are inefficient because of the memory that is required to store them. If each route is in the routing table, then any routing event (such as a flapping line) must be propagated throughout the network. Summarization limits the update traffic and minimizes the size of the routing tables of all routers. Configure the edge routers to announce a summary route of 10.x.0.0 255.255.0.0 to BBR1. Where do you place the appropriate command?
- Step 3** Review the routing table on BBR1 again. Remember that RIP is slow to converge. You may need to wait for up to a minute, even in this small network, before the summaries appear on BBR1. You may see many routes, but the relevant part of your display should resemble the following:

```
BBR1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is not set
    172.31.0.0/24 is subnetted, 2 subnets
C        172.31.3.0 is directly connected, Serial0/0.3
C        172.31.2.0 is directly connected, Serial0/0.2
          10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R        10.3.0.0/16 [120/1] via 172.31.3.2, 00:00:02,
Serial0/0.3
                                [120/1] via 172.31.3.1, 00:00:02,
Serial0/0.3
C        10.254.0.0/24 is directly connected, Ethernet0/0
```

- Step 4** Examine output from **show ip protocols** for details about the operation of RIP. Your display should resemble the following:

```
P3R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
```

```

      Interface          Send  Recv  Triggered RIP  Key-chain
Ethernet0/0            2     2
Serial0/0              2     2
Serial0/1              2     2

Automatic network summarization is not in effect

Address Summarization:
  10.3.0.0/16 for Serial0/0

Maximum path: 4

Routing for Networks:
  10.0.0.0
  172.31.0.0

Routing Information Sources:
  Gateway        Distance    Last Update
  10.3.0.1          120        00:00:19
  10.3.2.4          120        00:00:14
  172.31.3.1         120        00:00:20
  Gateway        Distance    Last Update
  172.31.3.3          120        00:00:01

Distance: (default is 120)

```

Exercise Verification

You have completed this exercise when you attain these results:

- You can set up RIPv2 and have full network visibility using RIPv2 as a routing protocol.
- You understand RIPv2 support for default routes, VLSM, and route summarization.
- You understand how VLSM contributes to network efficiency.

Lab Exercise 3-1: Configuring and Tuning EIGRP

Complete this lab exercise to practice what you learned in the related lesson.

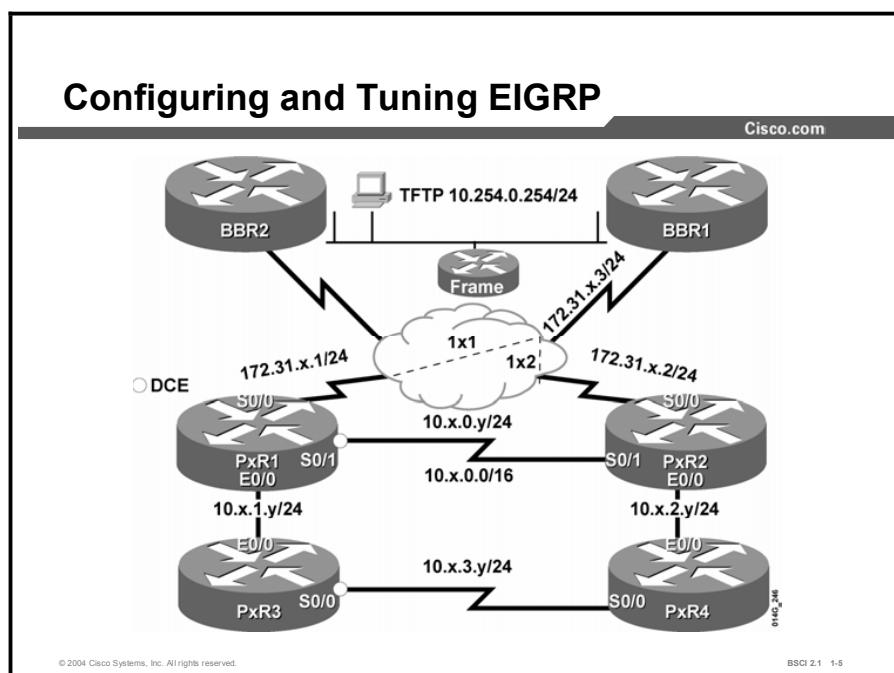
Exercise Objective

In this exercise, you will set up EIGRP and investigate its default behavior. Then you will optimize the EIGRP configuration. After completing this exercise, you will be able to meet these objectives:

- Recognize routes from the core and other pods using EIGRP
- Recognize EIGRP query traffic
- Configure route summarization using EIGRP
- Pass a default route in EIGRP
- Configure the EIGRP stub feature to limit the scope of the EIGRP queries

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
#debug ip eigrp	Displays EIGRP updates.
(config-router)#eigrp stub	Specifies that this router should behave as an “EIGRP stub” router.
(config-if)#ip summary-address eigrp 1 10.x.0.0 255.255.0.0	Creates and advertises a summary route out this interface.
(config-if)#ip summary-eigrp 1 0.0.0.0 0.0.0.0	Creates and advertises a default route out this interface and suppresses all other specific routes.
(config-router)#network 10.x.0.0 0.0.255.255	Specifies that EIGRP should run within network 10.3.0.0/16.
(config-router)#no auto-summary	Turns off automatic summarization at classful network boundaries.
(config)#router eigrp 1	Turns on EIGRP in AS 1.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

In this task, you will remove RIP before starting to investigate EIGRP. These instructions are the quickest way to do this. You may also simply copy the router setup file (PxRy.txt) to perform **startup-config** and **reload**. Be sure to copy the configuration of the internal router before reloading the edge router. After the router reloads, add the **ip classless** command.

Exercise Procedure

Complete these steps:

- Step 1** Remove all RIP commands and the static route from the edge routers. Your display should resemble the following:

```
P3R2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
P3R2(config)#no ip route 0.0.0.0 0.0.0.0 172.31.x.3  
P3R2(config)#no router rip  
P3R2(config)#int s0/0  
P3R2(config-if)#no ip summary-address rip 10.x.0.0 255.255.0.0  
P3R2(config-if)#end
```

- Step 2** Remove all RIP commands from the interior routers. Your display should resemble the following:

```
P3R4#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
P3R4(config)#no router rip  
P3R4(config)#end
```

Task 2: Configuring Basic EIGRP

In this task you will set up and investigate the operation of EIGRP.

Exercise Procedure

Complete these steps:

Step 1 Configure EIGRP on each router using AS number 1. Use appropriate network and wildcard values to include all interfaces in the EIGRP routing process. Disable autosummarization at the edge routers.

Step 2 Verify that the routers are set up correctly using **show ip protocols**. Make sure that the AS is correct and that all neighbors are exchanging routes. Your display should resemble the following:

```
P3R2#show ip protocols
Routing Protocol is "eigrp 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Default networks flagged in outgoing updates
    Default networks accepted from incoming updates
    EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    EIGRP maximum hopcount 100
    EIGRP maximum metric variance 1
    Redistributing: eigrp 1
    Automatic network summarization is not in effect
    Maximum path: 4
    Routing for Networks:
        10.3.0.0/16
        172.31.0.0/24
        172.31.3.0/24
    Routing Information Sources:
        Gateway          Distance      Last Update
        (this router)      90          00:03:04
        10.3.0.1          90          00:00:14
        10.3.2.4          90          00:00:14
        172.31.3.3        90          00:00:36
    Distance: internal 90 external 170
```

- Step 3** Verify that the remote routes are being recognized via EIGRP on each router. Your display should resemble the following:

```
P3R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.31.0.0/24 is subnetted, 2 subnets
C      172.31.3.0 is directly connected, Serial0/0
D      172.31.2.0 [90/21024000] via 172.31.3.3, 00:01:12,
Serial0/0
10.0.0.0/24 is subnetted, 5 subnets
D      10.3.1.0 [90/20537600] via 10.3.0.1, 00:00:50,
Serial0/1
C      10.3.0.0 is directly connected, Serial0/1
D      10.3.3.0 [90/20537600] via 10.3.2.4, 00:00:50,
Ethernet0/0
C      10.3.2.0 is directly connected, Ethernet0/0
D      10.254.0.0 [90/20537600] via 172.31.3.3, 00:01:12,
Serial0/0
```

- Step 4** Use **debug ip eigrp** on internal routers (PxR3 and PxR4) to monitor the EIGRP queries.

- Step 5** Shut down the serial interface between edge routers (the s0/1 interface on PxR1 and PxR2).

- Step 6** View the EIGRP queries that were sent to the internal routers. Your display should resemble the following:

```
IP-EIGRP Route Events debugging is on  
p6r4#debug ip eigrp
```

P6R4 receives query for network 10.6.0.0 from P6R2.

Network 10.6.0.0 is unreachable from P6R2 (infinite metric).

P6R4 replies to the query with network 10.6.0.0 unreachable (infinite metric).

```
1d12h: IP-EIGRP: Processing incoming QUERY packet
```

```
1d12h: IP-EIGRP: Int 10.6.0.0/24 M 4294967295 - 0 4294967295  
SM 4294967295 - 0 4294967295  
1d12h: IP-EIGRP: 10.6.0.0/24 routing table not updated  
1d12h: IP-EIGRP: 10.6.0.0/24 - do advertise out Ethernet0/0
```

```
1d12h: IP-EIGRP: Int 10.6.0.0/24 metric 4294967295 - 20000000  
4294967295
```

- Step 7** Turn off all debugging.

- Step 8** No shut the serial interface between edge routers (the s0/1 interface on PxR1 and PxR2).

Task 3: Configure EIGRP Core Scalability

In this task, you will configure EIGRP route summarizations. This configuration will add to the stability and speed convergence of the network by controlling the scope of queries, minimizing update traffic, and minimizing routing table size.

Exercise Procedure

Complete these steps:

- Step 1** Manually configure the edge routers (PxR1 and PxR2) to summarize the pod EIGRP routes to BBR1 into a single 10.x.0.0/16 advertisement (where x is your pod number).
- Step 2** Telnet to BBR1 (172.31.x.3) and verify that you see only the summary route and not the more specific routes from your pod. If both edge routers are correctly configured, you should see two equal-cost paths available to BBR1. Your display should resemble the following:

```
BBR1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
      * - candidate default, U - per-user static route, o -
ODR
      P - periodic downloaded static route

Gateway of last resort is not set
  172.31.0.0/24 is subnetted, 2 subnets
C        172.31.3.0 is directly connected, Serial0/0.3
C        172.31.2.0 is directly connected, Serial0/0.2
  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D          10.3.0.0/16 [90/20537600] via 172.31.3.1, 00:03:54,
Serial0/0.3
                                         [90/20537600] via 172.31.3.2, 00:03:54,
Serial0/0.3
C        10.254.0.0/24 is directly connected, Ethernet0/0
S        192.168.22.0/24 [1/0] via 172.31.2.2
S        192.168.2.0/24 [1/0] via 172.31.2.1
S        192.168.3.0/24 [1/0] via 172.31.3.1
S        192.168.33.0/24 [1/0] via 172.31.3.2
```

Task 4: Configuring the EIGRP Stub

Having optimized the routing table in the core BBRI router by summarizing the routes from the edge routers of the pod to the core BBR1 router, how can you now limit the query traffic from the edge routers of the pod to the internal routers of the pod?

Exercise Procedure

Complete these steps:

Step 1 Configure the internal routers (PxR3 and PxR4) as EIGRP stubs. Remember that this action bounds queries but does not affect the routing table.

Step 2 Verify that the edge router recognizes its internal EIGRP neighbor as a stub. Your display should resemble the following:

```
P5R2#show ip eigrp neighbors detail
IP-EIGRP neighbors for process 1
      H   Address             Interface   Hold Uptime   SRTT
      RTO  Q  Seq Type
                                         (sec)           (ms)
      Cnt Num
      2   10.5.2.4           Et0/0        14 00:03:24  880
      5000 0 96
          Version 12.1/1.2, Retrans: 0, Retries: 0
          Stub Peer Advertising ( CONNECTED SUMMARY ) Routes
          1   172.31.5.1         Se0/0        164 00:07:41  68
          1140 0 97
          Version 12.1/1.2, Retrans: 9, Retries: 0
          0   172.31.5.3         Se0/0        152 00:07:51  136
          1140 0 220
          Version 12.1/1.2, Retrans: 11, Retries: 0
P5R2#
```

Step 3 The stub designation bounds query traffic and helps avoid a situation called “stuck in active” (SIA), where EIGRP is unable to resolve routes for long periods. To demonstrate this situation, use the **debug ip eigrp** command on the internal router.

Step 4 Shut down the serial interface between the edge routers (the s0/1 interface between PxR1 and PxR2).

Step 5 Compared to before, when the internal routers were configured as stub, notice that no queries are now being sent to the internal router. You should *not* see the following debug message anymore after the internal routers are configured as a stub:

```
P3R4#
02:41:32: IP-EIGRP: Processing incoming QUERY packet
```

Step 6 Re-enable the serial interface between the edge routers (the s0/1 interface between PxR1 and PxR2).

Step 7 Turn off debugging on the internal routers (PxR3 and PxR4).

Task 5: Configuring the EIGRP Default Route

In this task, you will advertise a default route from the edge router to the internal router through EIGRP. This change will add to the stability and speed convergence of the network by minimizing update traffic and minimizing routing table size.

Exercise Procedure

Complete these steps:

Step 1 Send a default route from the edge router to the internal router. You also need to filter all specific routes. You can accomplish this step by configuring a summary route of 0.0.0.0 0.0.0.0 from the edge router to the internal router.

Step 2 Examine the routing table of the internal router. You will see the default route and connected routes and the EIGRP route that was learned from the other internal router, but the more specific routes that were received from the edge router have been filtered. Your display should resemble the following:

```
P3R4#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route

Gateway of last resort is 10.3.2.2 to network 0.0.0.0

          10.0.0.0/24 is subnetted, 3 subnets
D        10.3.1.0 [90/20537600] via 10.3.3.3, 00:00:04,
Serial0/0
C        10.3.3.0 is directly connected, Serial0/0
C        10.3.2.0 is directly connected, Ethernet0/0
D*      0.0.0.0/0 [90/307200] via 10.3.2.2, 00:00:04, Ethernet0/0
```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have successfully implemented EIGRP and see query traffic.
- You have summarized your pod to the core.
- You have optimized performance for the interior routers.

Lab Exercise 4-1: Configuring and Examining OSPF in a Single Area

Complete this lab exercise to practice what you learned in the related lesson.

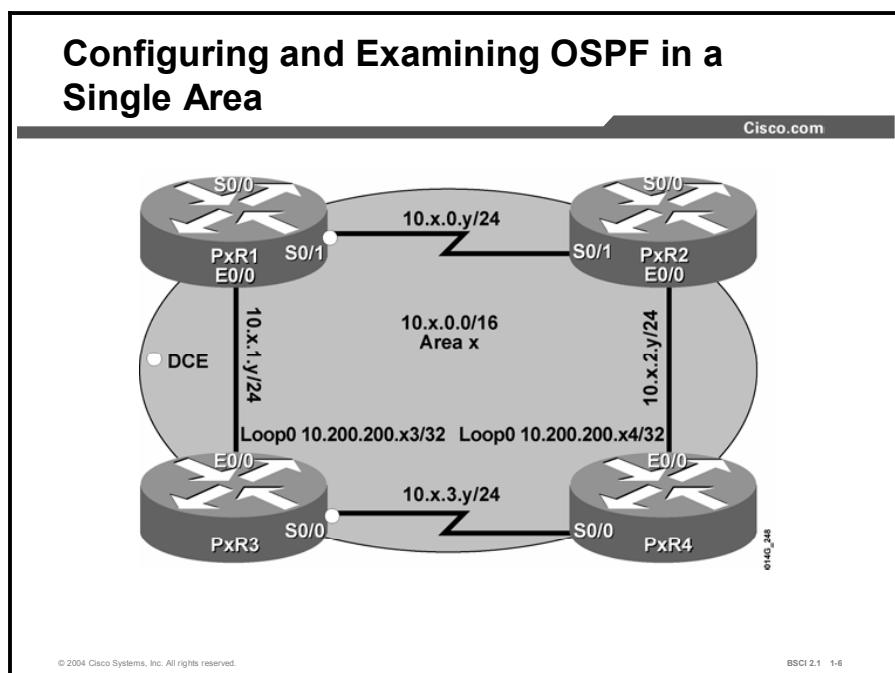
Exercise Objective

In this exercise, you will configure your pod as an OSPF single area. After completing this exercise, you will be able to meet these objectives:

- Configure OSPF for a single area
- Configure a stable OSPF router ID

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Note Throughout the exercise the pod number is referred to with x and the router number with y. Substitute the appropriate number as needed.

Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4). These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers

This lab exercise requires the topology internal to the pod. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
#clear ip ospf process	Resets the OSPF process.
#debug ip ospf events	Views OSPF process evolution.
#debug ip ospf events	Views OSPF process.
#show ip ospf	Views OSPF process parameters.
#show ip ospf neighbor	Views all OSPF neighbors.
(config)#router ospf 1	Turns on OSPF. The process number is not communicated to other routers.
(config-if)#ip ospf priority 0	Removes a router from contention as a DR or BDR.
(config-router)#network 10.x.0.0 0.0.255.255 area 1	Specifies interfaces on which OSPF will run.
(config-router)#router-id 10.0.0.xy	Configures the OSPF router ID (RID).

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

Before starting to investigate OSPF, you need to remove Enhanced Interior Gateway Routing Protocol (EIGRP).

Exercise Procedure

Complete these steps:

- Step 1** Disable EIGRP on the routers. Your display should resemble the following:

```
P1R2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
P1R2(config)#no router eigrp 1  
P1R2(config)#end
```

- Step 2** You may also simply copy the router setup file (PxRy.txt) to perform **startup-config** and **reload**. After the router restarts, you also need to add the command **ip classless**.

- Step 3** If access to the TFTP server is not available, you should erase the startup-configuration and reload. Type in the necessary commands. The configuration for the edge routers follows:

```
host PxRy  
no ip domain-lookup  
ip classless  
enable password cisco  
line con 0  
logging synchronous  
exec-timeout 30 0  
line vty 0 4  
no login  
exit  
int s0/0  
ip address 172.31.1.2 255.255.255.0  
encapsulation frame-relay  
shutdown  
no fair-queue  
frame-relay map ip 172.31.1.3 112 broadcast  
no frame-relay inverse-arp  
int s0/1  
ip address 10.x.0.y 255.255.255.0  
clock rate 64000  
no shutdown  
int e0/0  
ip address 10.x.y.y 255.255.255.0
```

```
no shutdown
```

```
end
```

The configuration for the internal routers follows:

```
host PxRy
no ip domain-lookup
ip classless
enable password cisco
line con 0
logging synchronous
exec-timeout 30 0
line vty 0 4
no login
exit
int e 0/0
ip address 10.x.(y-2).y 255.255.255.0
no shut
int s0/0
ip address 10.x.3.y 255.255.255.0
clock rate 64000
no shut
end
```

Task 2: Configuring Single Area OSPF Within Your Pod

In this task you will configure a single area OSPF within your own pod.

Exercise Procedure

Complete these steps:

- Step 1** Shut down the Frame Relay connection (serial 0/0 on edge routers PxR1 and PxR2).
- Step 2** Configure OSPF on the pod routers as area x , where x is your pod number. To avoid problems in a later lab, use a network statement for your pod network 10.x.0.0, rather than the entire 10.0.0.0 network.

Step 3 Use the proper **show** command to verify the OSPF RID on the pod routers. The RID is the highest active IP address on the router. Notice that R1 and R2 have not chosen their Frame Relay IP addresses because those interfaces are not active.

What is the OSPF RID of your pod routers, and is it what you expected the RID to be?

RID of PxR1: _____

RID of PxR2: _____

RID of PxR3: _____

RID of PxR4: _____

Step 4 Configure a loopback 0 interface on PxR3 and PxR4 with the IP address 10.200.200.xy /32, where x is your pod number and y is the router number.

Step 5 Use the proper **show** command to verify the OSPF RID on the internal router. The RID is supposed to be the highest loopback address or, if there is no loopback address, the highest active address.

What is the OSPF RID of your pod internal routers now, and is it what you expected the RID to be?

RID of PxR3: _____

RID of PxR4: _____

Step 6 Notice that in the previous step the RID did not change; this is a stability feature of Cisco IOS software. If the RID changed, the link-state advertisements (LSAs) would be invalid and the router would have to reconverge. Reload the internal routers to get the RID to change because the loopback interface was configured after the OSPF process was configured.

Step 7 Use the proper **show** command to verify that the RID has changed to the loopback 0 interface after the internal routers reloaded.

Step 8 On the PxR1 and PxR2 routers, set the OSPF RID to 10.0.0.xy, where x is your pod number and y is the router number, using the **router-id** command in OSPF router configuration mode.

Step 9 Reset the OSPF process with the privilege mode command **clear ip ospf process** to make the **router-id** command take effect. The **router-id** command is another way to set the OSPF RID. This command was introduced in Cisco IOS Release 12.0(1)T.

Note To change the OSPF ID of a router by configuring a loopback interface requires either a reboot of the router, or the disabling and then enabling of OSPF. To change an OSPF ID of a router by configuring the RID under the OSPF process requires only that the OSPF process be cleared, a much less drastic move.

Step 10 Use the proper **show** command to verify that the RID of the edge router has changed to 10.0.0.xy after the OSPF process reset.

Step 11 Before finishing, make sure that all neighbors are in communication (in the FULL state) on all your pod routers. This action will avoid problems in future labs.

Step 12 Display the IP routing table to be sure that you are getting OSPF routes.

Task 3: Understanding OSPF Packet Types

Step 1 Examine OSPF packet types with the **debug ip ospf events** command.

Step 2 Reset the OSPF process and examine OSPF adjacency building and election of a DR and a BDR. Your display should resemble the following:

A hello is received.

```
p5r1#debug ip ospf events
OSPF events debugging is on
p5r1#clear ip ospf process
2w3d: OSPF: Rcv hello from 10.0.0.52 area 5 from Serial0/1
10.5.0.2
2w3d: OSPF: End of hello processing
Reset ALL OSPF processes? [no] : yes
p5r1#
p5r1#
2w3d: OSPF: Flushing External Links
2w3d: OSPF: Flushing Opaque AS Links
2w3d: OSPF: Flushing Link states in area 5
2w3d: OSPF: Interface Serial0/1 going Down
2w3d: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.52 on Serial0/1
from FULL to DOWN, N
Neighbor Down: Interface down or detached
2w3d: OSPF: Interface Ethernet0/0 going Down
2w3d: OSPF: Neighbor change Event on interface Ethernet0/0
DR election
2w3d: OSPF: DR/BDR election on Ethernet0/0
2w3d: OSPF: Elect BDR 0.0.0.0
2w3d: OSPF: Elect DR 10.200.200.53
2w3d: OSPF: Elect BDR 0.0.0.0
2w3d: OSPF: Elect DR 10.200.200.53
2w3d: DR: 10.200.200.53 (Id) BDR: none
2w3d: %OSPF-5-ADJCHG: Process 1, Nbr 10.200.200.53 on
Ethernet0/0 from FULL to D
OWN, Neighbor Down: Interface down or detached
2w3d: OSPF: Neighbor change Event on interface Ethernet0/0
2w3d: OSPF: DR/BDR election on Ethernet0/0
2w3d: OSPF: Elect BDR 0.0.0.0
2w3d: OSPF: Elect DR 0.0.0.0
2w3d: DR: none BDR: none
2w3d: OSPF: Remember old DR 10.200.200.53 (id)
```

```

2w3d: OSPF: Interface Serial0/1 going Up
2w3d: OSPF: Interface Ethernet0/0 going Up
2w3d: OSPF: Rcv hello from 10.200.200.53 area 5 from
Ethernet0/0 10.5.1.3
2w3d: OSPF: 2 Way Communication to 10.200.200.53 on
Ethernet0/0, state 2WAY
2w3d: OSPF: Backup seen Event before WAIT timer on Ethernet0/0
2w3d: OSPF: DR/BDR election on Ethernet0/0
2w3d: OSPF: Elect BDR 10.0.0.51
BDR election 2w3d: OSPF: Elect DR 10.200.200.53
2w3d: OSPF: Elect BDR 10.0.0.51
2w3d: OSPF: Elect DR 10.200.200.53
2w3d: DR: 10.200.200.53 (Id) BDR: 10.0.0.51 (Id)
2w3d: OSPF: Send DBD to 10.200.200.53 on Ethernet0/0 seq 0x306
opt 0x42 flag 0x7
len 32
2w3d: OSPF: End of hello processing
Exstart: Who will
lead the database
description (DBD)
exchange? 2w3d: OSPF: Rcv DBD from 10.200.200.53 on Ethernet0/0 seq
0x231A opt 0x42 flag 0
x7 len 32 mtu 1500 state EXSTART
2w3d: OSPF: NBR Negotiation Done. We are the SLAVE
2w3d: OSPF: Send DBD to 10.200.200.53 on Ethernet0/0 seq
0x231A opt 0x42 flag 0x
0 len 32
2w3d: OSPF: Rcv DBD from 10.200.200.53 on Ethernet0/0 seq
0x231B opt 0x42 flag 0
x3 len 132 mtu 1500 state EXCHANGE
2w3d: OSPF: Send DBD to 10.200.200.53 on Ethernet0/0 seq
0x231B opt 0x42 flag 0x
0 len 32
2w3d: OSPF: Database request to 10.200.200.53
2w3d: OSPF: sent LS REQ packet to 10.5.1.3, length 60
2w3d: OSPF: Rcv DBD from 10.200.200.53 on Ethernet0/0 seq
0x231C opt 0x42 flag 0
x1 len 32 mtu 1500 state EXCHANGE
2w3d: OSPF: Exchange Done with 10.200.200.53 on Ethernet0/0
2w3d: OSPF: Send DBD to 10.200.200.53 on Ethernet0/0 seq
0x231C opt 0x42 flag 0x
0 len 32
2w3d: OSPF: Synchronized with 10.200.200.53 on Ethernet0/0,
state FULL
2w3d: %OSPF-5-ADJCHG: Process 1, Nbr 10.200.200.53 on
Ethernet0/0 from LOADING t
o FULL, Loading Done

```

```

2w3d: OSPF: Rcv hello from 10.0.0.52 area 5 from Serial0/1
10.5.0.2

2w3d: OSPF: 2 Way Communication to 10.0.0.52 on Serial0/1,
state 2WAY

2w3d: OSPF: Send DBD to 10.0.0.52 on Serial0/1 seq 0x20AD opt
0x42 flag 0x7 len
32

2w3d: OSPF: End of hello processing

2w3d: OSPF: Rcv DBD from 10.0.0.52 on Serial0/1 seq 0x12DB opt
0x42 flag 0x7 len
32 mtu 1500 state EXSTART

2w3d: OSPF: NBR Negotiation Done. We are the SLAVE

2w3d: OSPF: Send DBD to 10.0.0.52 on Serial0/1 seq 0x12DB opt
0x42 flag 0x2 len
152

Exchange state:
trading DBDs

2w3d: OSPF: Rcv DBD from 10.0.0.52 on Serial0/1 seq 0x12DC opt
0x42 flag 0x3 len
152 mtu 1500 state EXCHANGE

2w3d: OSPF: Send DBD to 10.0.0.52 on Serial0/1 seq 0x12DC opt
0x42 flag 0x0 len
32

2w3d: OSPF: Rcv DBD from 10.0.0.52 on Serial0/1 seq 0x12DD opt
0x42 flag 0x1 len
32 mtu 1500 state EXCHANGE

2w3d: OSPF: Exchange Done with 10.0.0.52 on Serial0/1
2w3d: OSPF: Synchronized with 10.0.0.52 on Serial0/1, state
FULL

Full state indicates
that the exchange is
complete.

2w3d: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.52 on Serial0/1
from LOADING to FULL
, Loading Done

2w3d: OSPF: Send DBD to 10.0.0.52 on Serial0/1 seq 0x12DD opt
0x42 flag 0x0 len
32

p5r1#
p5r1#

2w3d: OSPF: Rcv hello from 10.200.200.53 area 5 from
Ethernet0/0 10.5.1.3

2w3d: OSPF: Neighbor change Event on interface Ethernet0/0
2w3d: OSPF: DR/BDR election on Ethernet0/0
2w3d: OSPF: Elect BDR 10.0.0.51
2w3d: OSPF: Elect DR 10.200.200.53
2w3d: DR: 10.200.200.53 (Id) BDR: 10.0.0.51 (Id)
2w3d: OSPF: End of hello processing
p5r1#

```

Task 4: Understanding OSPF DR and BDR elections

In this task you will examine the OSPF DR and BDR elections.

Exercise Procedure

- Step 1** Determine the default OSPF priority and which router is the DR on the Ethernet segment using the **show ip ospf neighbor** command.
- Step 2** Change the DR by adjusting the OSPF priority to 0 for the appropriate routers on the Ethernet interface. This removes the current DR from the election process. Observe the results when the edge router is elected as the DR (**debug ip ospf events** is still running):

```
01:37:10: OSPF: Neighbor change Event on interface Ethernet0/0
01:37:10: OSPF: DR/BDR election on Ethernet0/0
01:37:10: OSPF: DR/BDR election on Ethernet0/0
01:37:10: OSPF: Elect DR 10.0.0.12
01:37:10: OSPF: Elect BDR 10.0.0.12
01:37:10: OSPF: Elect DR 10.0.0.12
01:37:10:     DR: 10.0.0.12 (Id)     BDR: 10.0.0.12 (Id)
01:37:10: OSPF: Set Ethernet0/0 flush timer
01:37:10: OSPF: Remember old DR 10.200.200.14 (id)
01:37:16: OSPF: Rcv hello from 10.0.0.12 area 1 from
Ethernet0/0 10.1.2.2
01:37:16: OSPF: End of hello processing
01:37:19: OSPF: Rcv hello from 10.200.200.3 area 1 from
Serial0/0 10.1.3.3
01:37:19: OSPF: End of hello processing
01:37:26: OSPF: Rcv hello from 10.0.0.12 area 1 from
Ethernet0/0 10.1.2.2
01:37:26: OSPF: Neighbor change Event on interface Ethernet0/0
01:37:26: OSPF: DR/BDR election on Ethernet0/0
01:37:26: OSPF: Elect BDR 0.0.0.0
01:37:26: OSPF: Elect DR 10.0.0.12
01:37:26:     DR: 10.0.0.12 (Id)     BDR: none
01:37:26: OSPF: End of hello processing
01:37:29: OSPF: Rcv hello from 10.200.200.3 area 1 from
Serial0/0 10.1.3.3
01:37:29: OSPF: End of hello processing
01:37:36: OSPF: Rcv hello from 10.0.0.12 area 1 from
Ethernet0/0 10.1.2.2
01:37:36: OSPF: End of hello processing
01:37:39: OSPF: Rcv hello from 10.200.200.3 area 1 from
Serial0/0 10.1.3.3
```

- Step 3** Once you have seen the DR and BDR election, turn off the debug.

Step 4 Verify the results of the election by displaying the neighbor database:

```
p5r2#show ip ospf neighbor
Neighbor ID      Pri      State            Dead Time   Address
Interface
10.200.200.54    0        FULL/DROTHER    00:00:34
10.5.2.4          Ethernet0/0
10.0.0.51         1        FULL/           -          00:00:30
10.5.0.1          Serial0/1
```

Exercise Verification

You have completed this exercise when you attain these results:

- EIGRP is removed from the routers.
- OSPF is running, and all pod routes are being passed.
- You understand how to control the RID.
- You can witness OSPF neighborship formation.
- You can administratively determine the DR and BDR.

Lab Exercise 4-2: Configuring OSPF for Multiple Areas and Frame Relay NBMA

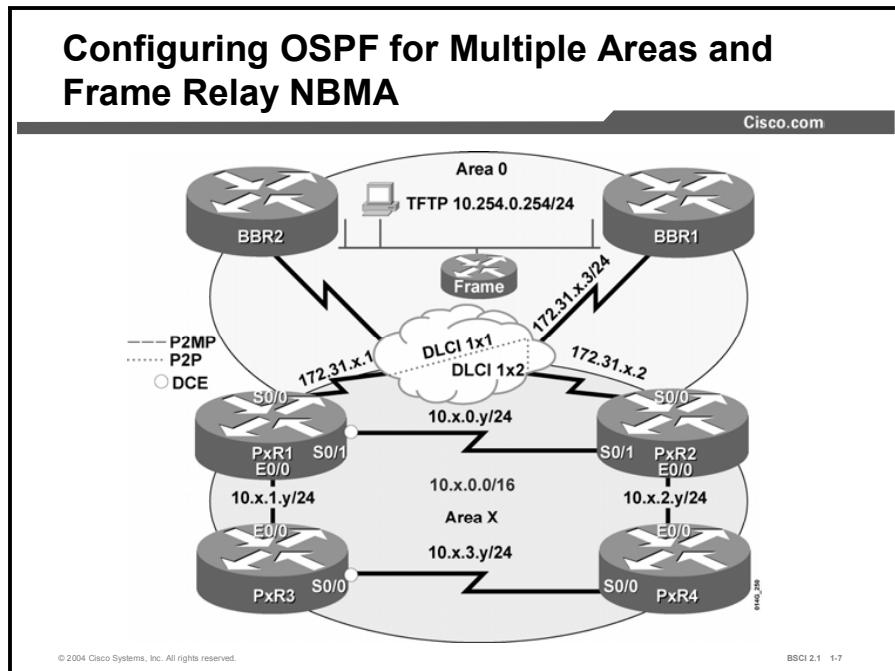
Complete this lab exercise to practice what you learned in the related lesson.

Exercise Objective

In this exercise, you will configure OSPF for use over simple Frame Relay networks. After completing this exercise, you will be able to meet these objectives:

- Configure OSPF in an NBMA network
- Configure OSPF in a multiarea environment

Visual Objective



Required Resources

These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (BBR1) configured for OSPF routing with the pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4 and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-if) #ip ospf priority 0	Sets the OSPF priority of a port to 0 to prevent it from participating in DR and BDR election.
(config-router) #network 172.31.x.0 0.0.0.255 area 0	Places a set of interfaces in an OSPF area.

Job Aids

There are no job aids for this lab exercise.

Task 1: Using the Nonbroadcast OSPF Network Type over Frame Relay

In this task, the learner configures ABRs, allowing OSPF to pass routes between areas.

Exercise Procedure

Complete these steps:

- Step 1** Configure the edge routers (PxR1 and PxR2) as ABRs. This task is done by placing the Frame Relay connection (the s0/0 interface on the edge routers) into OSPF area 0. Remember that the default OSPF network type for a Frame Relay interface is NBMA (nonbroadcast).
- Step 2** It is important that the core (BBR1) is the DR because this is a hub-and-spoke network and only the core (BBR1) has full connectivity to the spoke routers. Set the OSPF priority to 0 on the s0/0 interface of the edge routers to ensure this designation.

Note In an NBMA network, neighbor statements are required only on the DR and BDR. In the hub-and-spoke topology, neighbor statements must be configured on the hub (which must become the DR) and are not mandatory on the spoke routers. However, in a full-mesh topology, you may need neighbor statements on all routers if you have not specified the DR and BDR with the **priority** command.

- Step 3** Enable serial 0/0 interfaces on edge routers with the **no shut** command (it was still down from the previous lab).
- Step 4** View the routing table on the internal routers to ensure that all appropriate OSPF routes are present and ping the TFTP server from the internal router to verify network connectivity. What is the difference between the O, O IA, and O E2 OSPF routes?

Your **show ip route** output should resemble the following:

```
p1r4#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is not set
          172.31.0.0/24 is subnetted, 6 subnets
```

```

O IA      172.31.3.0 [110/1572] via 10.1.2.2, 00:00:07,
Ethernet0/0

O IA      172.31.2.0 [110/1572] via 10.1.2.2, 00:00:07,
Ethernet0/0

O IA      172.31.1.0 [110/791] via 10.1.2.2, 00:00:07,
Ethernet0/0

O IA      172.31.6.0 [110/1572] via 10.1.2.2, 00:00:07,
Ethernet0/0

O IA      172.31.5.0 [110/1572] via 10.1.2.2, 00:00:07,
Ethernet0/0

O IA      172.31.4.0 [110/1572] via 10.1.2.2, 00:00:07,
Ethernet0/0

          10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.3.0/24 is directly connected, Serial0/0
C        10.1.2.0/24 is directly connected, Ethernet0/0
O        10.1.1.0/24 [110/791] via 10.1.3.3, 00:01:08,
Serial0/0
O        10.1.0.0/24 [110/791] via 10.1.2.2, 00:01:08,
Ethernet0/0
C        10.200.200.14/32 is directly connected, Loopback0
O E2      10.254.0.0/24 [110/50] via 10.1.2.2, 00:00:05,
Ethernet0/0

```

- Step 5** At the edge routers, verify OSPF neighborship with the command **show ip ospf neighbor**. Is BBR1 the DR for the 172.31.x.0/24 hub-and-spoke network?
- Step 6** BBR1 has been configured with neighbor statements for each of the edge routers. Telnet to BBR1 (172.31.x.3) and view the running configuration to verify the neighbor statements for the edge routers of your pod, PxR1 and PxR2. Close the Telnet connection.
- Step 7** On the pod edge routers, PxR1 and PxR2, verify the OSPF network type of the Frame Relay interface.

What is the OSPF network type on the Frame Relay interface?

On the HDLC serial interface between PxR1 and PxR2?

On the Ethernet interface?

Remember these key differences in OSPF NBMA network types:

Network Type	Specify Neighbors	DR	Topology Required	Hello Interval	Notes
NBMA	YES	YES	Full-mesh	30	If not full-mesh, at least the DR and BDR need to have full physical connectivity with all routers that exist in the cloud.
Point-to-multipoint	NO	NO	Arbitrary	30	
Broadcast	NO	YES	Full-mesh	10	If not full-mesh, at least the DR and BDR need to have full physical connectivity with all routers that exist in the cloud.
Point-to-point	NO	NO	Point-to-point	10	

Your display should resemble the following:

```
P1R1#show ip ospf interface
Ethernet0/0 is up, line protocol is up
    Internet Address 10.1.1.1/24, Area 1
    Process ID 1, Router ID 10.0.0.11, Network Type BROADCAST,
Cost: 10
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 10.0.0.11, Interface address 10.1.1.1
        No backup designated router on this network
        Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
            Hello due in 00:00:03
            Index 1/1, flood queue length 0
            Next 0x0(0)/0x0(0)
            Last flood scan length is 7, maximum is 7
            Last flood scan time is 0 msec, maximum is 0 msec
            Neighbor Count is 1, Adjacent neighbor count is 1
                Adjacent with neighbor 10.200.200.3
                Suppress hello for 0 neighbor(s)
Serial0/0 is up, line protocol is up
    Internet Address 172.31.1.1/24, Area 0
    Process ID 1, Router ID 10.0.0.11, Network Type
NON_BROADCAST, Cost: 781
        Transmit Delay is 1 sec, State DROTHER, Priority 0
        Designated Router (ID) 100.100.100.100, Interface address
172.31.1.3
        No backup designated router on this network
```

```

        Timer intervals configured, Hello 30, Dead 120, Wait 120,
        Retransmit 5

        Hello due in 00:00:23
        Index 1/3, flood queue length 0
        Next 0x0(0)/0x0(0)
        Last flood scan length is 1, maximum is 1
        Last flood scan time is 0 msec, maximum is 0 msec
        Neighbor Count is 1, Adjacent neighbor count is 1
            Adjacent with neighbor 100.100.100.100  (Designated
Router)

            Suppress hello for 0 neighbor(s)

Serial0/1 is up, line protocol is up
    Internet Address 10.1.0.1/24, Area 1
    Process ID 1, Router ID 10.0.0.11, Network Type
POINT_TO_POINT, Cost: 781
    Transmit Delay is 1 sec, State POINT_TO_POINT,
    Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Retransmit 5

        Hello due in 00:00:07
        Index 2/2, flood queue length 0
        Next 0x0(0)/0x0(0)
        Last flood scan length is 6, maximum is 6
        Last flood scan time is 0 msec, maximum is 0 msec
        Neighbor Count is 1, Adjacent neighbor count is 1
            Adjacent with neighbor 10.0.0.12

            Suppress hello for 0 neighbor(s)

```

Exercise Verification

You have completed this exercise when you attain these results:

- You have enabled OSPF to the core.
- You have a full set of OSPF routes in your routing tables.
- You can ping the core TFTP server.

Lab Exercise 4-3: Configuring OSPF for Multiple Areas and Frame Relay Point-to-Multipoint and Point-to-Point

Complete this lab exercise to practice what you learned in the related lesson.

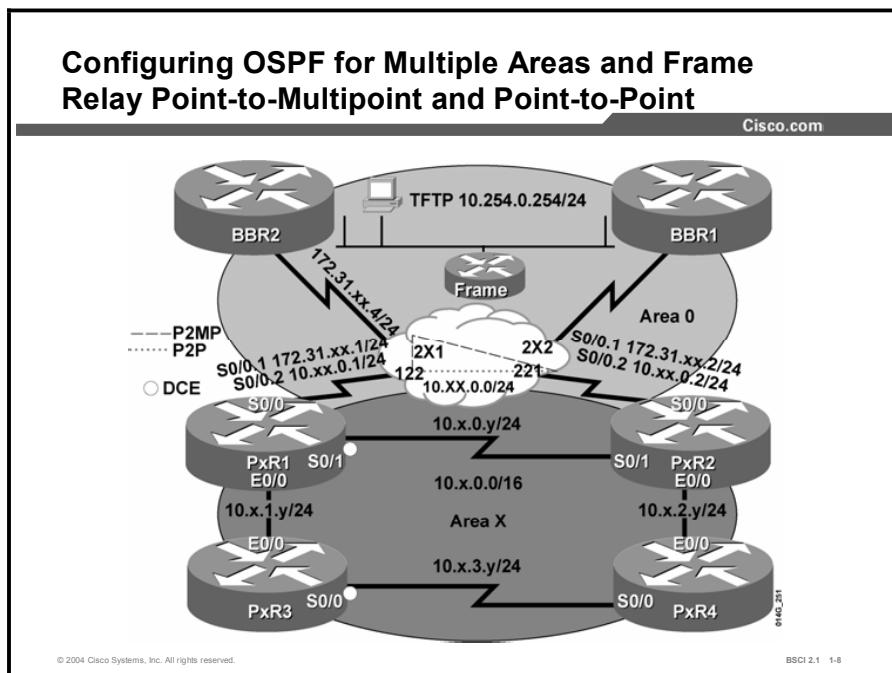
Exercise Objective

In this exercise, you will configure OSPF for use over complex Frame Relay networks. After completing this exercise, you will be able to meet these objectives:

- Configure OSPF over Frame Relay using the point-to-multipoint OSPF network type
- Configure OSPF over Frame Relay using the point-to-point OSPF network type
- Connect to other devices in the core

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (BBR2) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4 and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config)#default interface s0/0	Erases the configuration on an interface.
(config-subif)#frame-relay interface-dlci 122	Specifies the DLCI that is associated with this point-to-point link.
(config)#interface s0/0.1 multipoint point-to-point	Creates a subinterface (either multipoint or point-to-point).
(config-subif)#ip ospf network point-to-multipoint	Forces OSPF to treat this interface as point-to-multipoint; the default is NBMA.
(config-router)#network 172.31.0.0 0.0.255.255 area 0	Sets interfaces that match this pattern to be in this OSPF area.
(config-if)#no frame-relay inverse-arp	Disables Frame Relay inverse Address Resolution Protocol (ARP) on the interface.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

In this task, you will prepare the interface s0/0 on the edge routers for use in the following tasks.

Exercise Procedure

Complete these steps:

- Step 1** Shut the Frame Relay interface, serial 0/0, on the edge routers. In order to prepare the interface for use in this lab, make the following interface configuration changes:

Remove all Frame Relay map statements
Remove the IP address
Remove the OSPF priority statement

Alternatively, you may remove the entire configuration from the interface by issuing the command **default interface s0/0**.

- Step 2** View the running configuration to verify that the s0/0 interface of the edge routers is configured to use Frame Relay encapsulation and that **frame-relay inverse-arp** is disabled.

If you have used the **default interface s0/0** command, enable Frame Relay encapsulation on the serial 0/0 interface. Turn off **frame-relay inverse-arp** on that interface.

Task 2: Configuring OSPF for Multiple Areas and Frame Relay Point-to-Multipoint and Point-to-Point

In this task you will configure OSPF for multiple areas and the Frame Relay point-to-multipoint and point-to-point.

Exercise Procedure

Note	For this lab, you will connect the edge routers to the BBR2 router over the 172.31.xx.0/24 network. The connection from the edge routers to the BBR1 router over the 172.31.x.0/24 network will not be used.
-------------	--

Complete these steps:

- Step 1** At the edge routers, create a multipoint subinterface numbered s0/0.1. You will use this interface to explore Frame Relay hub-and-spoke behavior using the OSPF point-to-multipoint network type.
- Step 2** Change the s0/0.1 OSPF network type to point-to-multipoint (the default OSPF network type for a Frame Relay multipoint subinterface is nonbroadcast).
- Step 3** Assign the IP address 172.31.xx.y/24 to s0/0.1, where x is the pod number and y is the router number. For example, for P3R2, the IP address will be 172.31.33.2/24.

- Step 4** Because you are not using **frame relay inverse arp**, you need to manually map the remote IP address to the local DLCI. Create a new Frame Relay map statement from each edge router to the BBR2 IP address of 172.31.xx.4 using a DLCI number of 2xy, where x is the pod number and y is the router number. Do not forget the broadcast option.

For example, for P3R2, the Frame Relay map statement will be the following:

```
frame-relay map ip 172.31.33.4 232 broadcast
```

And for P3R1, the Frame Relay map statement will be the following:

```
frame-relay map ip 172.31.33.4 231 broadcast
```

- Step 5** No shut the serial 0/0 interface on the edge routers.

- Step 6** At the edge routers, add a new network statement to OSPF for the 172.31.xx.0 network that has been created on s0/0.1, placing it in Area 0.

- Step 7** On the edge routers, use the proper **show** command to display the OSPF neighbor status. Is there a DR or BDR using the point-to-multipoint OSPF network type? Your display should resemble the following:

```
P3R1#show ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface
10.200.200.33    0     FULL/DROTHER   00:00:35      10.3.1.3
Ethernet0/0
200.200.200.200  1     FULL/      -       00:01:57      172.31.33.4
Serial0/0.1
10.0.0.321        FULL/      -       00:00:35      10.3.0.2
Serial0/1
P3R1#
```

- Step 8** View the routing table on the edge routers PxR1 and PxR2 to verify that they are receiving OSPF routes from the core.

Ping the Ethernet interface of BBR2 (10.254.0.2) from the edge routers to verify connectivity with the core. Your output should resemble the following:

```
P5R1#ping 10.254.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.254.0.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/33/36 ms
```

- Step 9** Create a new point-to-point subinterface to connect the two edge routers. Give the new subinterface the number s0/0.2. Address it as 10.xx.0.y/24, where x is the pod number and y is the router number. The DLCI from PxR1 to PxR2 is 122, and the DLCI from PxR2 to PxR1 is 221, in every pod.

For example, for P3R1 and P3R2, the configuration should be as follows:

```
P3R1(config)#interface s0/0.2 point-to-point
P3R1(config-subif)#ip address 10.33.0.1 255.255.255.0
P3R1(config-subif)#frame-relay interface-dlci 122
P3R2(config)#interface s0/0.2 point-to-point
P3R2(config-subif)#ip address 10.33.0.2 255.255.255.0
P3R2(config-subif)#frame-relay interface-dlci 221
```

- Step 10** At each edge router, ping the s0/0.2 subinterface of the other edge router to verify connectivity. Your output should resemble the following:

```
P5R1#ping 10.55.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.55.0.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
32/33/36 ms
p5r1#
```

- Step 11** At the edge routers, add the 10.xx.0.0 network to OSPF in area x.

- Step 12** At the edge routers, verify the OSPF network type of the two subinterfaces. What is the default OSPF network type on the point-to-point subinterface? Your display should resemble the following:

```
P3R1#sh ip ospf interface
[output omitted]
Serial0/0.1 is up, line protocol is up
    Internet Address 172.31.33.1/24, Area 0
    Process ID 1, Router ID 10.3.1.1, Network Type
    POINT_TO_MULTIPOINT, Cost: 781
    Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
    Timer intervals configured, Hello 30, Dead 120, Wait 120,
    Retransmit 5
    Hello due in 00:00:05
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 200.200.200.200
```

```

        Suppress hello for 0 neighbor(s)
Serial0/0.2 is up, line protocol is up
        Internet Address 10.33.0.1/24, Area 3
        Process ID 1, Router ID 10.3.1.1, Network Type
POINT_TO_POINT, Cost: 781
        Transmit Delay is 1 sec, State POINT_TO_POINT,
        Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
        Hello due in 00:00:09
        Index 1/4, flood queue length 0
        Next 0x0(0)/0x0(0)
        Last flood scan length is 1, maximum is 24
        Last flood scan time is 0 msec, maximum is 0 msec
        Neighbor Count is 1, Adjacent neighbor count is 1
        Adjacent with neighbor 10.3.2.2
        Suppress hello for 0 neighbor(s)
[output omitted]

```

- Step 13** At the edge routers, use the proper **show** command to verify the OSPF neighbor status.

Is there a DR or BDR on s0/0.2 using the point-to-point OSPF network type?

Your display should resemble the following:

```

P3R2# sh ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface

10.200.200.34    0     FULL/DROTHER   00:00:35     10.3.2.4
Ethernet0/0

200.200.200.200  1     FULL/          -           00:01:42     172.31.33.4
Serial0/0.1

10.0.0.31         1     FULL/          -           00:00:36     10.33.0.1
Serial0/0.2

10.0.0.31         1     FULL/          -           00:00:35     10.3.0.1
Serial0/1

```

- Step 14** At the edge routers, verify the OSPF routes in the IP routing table. You may not see routes from every pod, depending on the number of pods in use in the class.

```

P5R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP

```

```

        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
        * - candidate default, U - per-user static route, o -
ODR
        P - periodic downloaded static route
Gateway of last resort is not set
    172.31.0.0/16 is variably subnetted, 8 subnets, 2 masks
O      172.31.55.4/32 [110/781] via 172.31.55.4, 00:04:35,
Serial0/0.1
C      172.31.55.0/24 is directly connected, Serial0/0.1
O      172.31.55.1/32 [110/1562] via 172.31.55.4, 00:04:35,
Serial0/0.1
O      172.31.33.4/32 [110/781] via 172.31.55.4, 00:04:35,
Serial0/0.1
O      172.31.44.4/32 [110/781] via 172.31.55.4, 00:04:35,
Serial0/0.1
O      172.31.22.4/32 [110/781] via 172.31.55.4, 00:04:35,
Serial0/0.1
O      172.31.11.4/32 [110/781] via 172.31.55.4, 00:04:36,
Serial0/0.1
O      172.31.66.4/32 [110/781] via 172.31.55.4, 00:04:36,
Serial0/0.1
        10.0.0.0/24 is subnetted, 6 subnets
O      10.5.3.0 [110/791] via 10.5.2.4, 00:04:36, Ethernet0/0
C      10.5.2.0 is directly connected, Ethernet0/0
O      10.5.1.0 [110/791] via 10.5.0.1, 00:04:36, Serial0/1
C      10.5.0.0 is directly connected, Serial0/1
C      10.55.0.0 is directly connected, Serial0/0.2
O E2   10.254.0.0 [110/50] via 172.31.55.4, 00:04:27,
Serial0/0.1

```

Step 15 At the interior routers, verify the OSPF routes in the IP routing table.

Why are some routes marked “O IA” on the internal router, but not at the edge?

```

P5R4>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
        * - candidate default, U - per-user static route, o -
ODR

```

```

P - periodic downloaded static route
Gateway of last resort is not set
    172.31.0.0/32 is subnetted, 8 subnets
O IA    172.31.55.4 [110/791] via 10.5.2.2, 00:04:50,
Ethernet0/0
O IA    172.31.55.1 [110/791] via 10.5.2.2, 00:04:50,
Ethernet0/0
                                                [110/791] via 10.5.3.3, 00:04:50,
Serial0/0
O IA    172.31.55.2 [110/10] via 10.5.2.2, 00:04:50,
Ethernet0/0
O IA    172.31.33.4 [110/791] via 10.5.2.2, 00:04:50,
Ethernet0/0
O IA    172.31.44.4 [110/791] via 10.5.2.2, 00:04:50,
Ethernet0/0
O IA    172.31.22.4 [110/791] via 10.5.2.2, 00:04:50,
Ethernet0/0
O IA    172.31.11.4 [110/791] via 10.5.2.2, 00:04:52,
Ethernet0/0
O IA    172.31.66.4 [110/791] via 10.5.2.2, 00:04:52,
Ethernet0/0
        10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C      10.5.3.0/24 is directly connected, Serial0/0
C      10.5.2.0/24 is directly connected, Ethernet0/0
O      10.5.1.0/24 [110/791] via 10.5.3.3, 00:04:54,
Serial0/0
O      10.5.0.0/24 [110/791] via 10.5.2.2, 00:04:54,
Ethernet0/0
C      10.200.200.54/32 is directly connected, Loopback1
O      10.55.0.0/24 [110/791] via 10.5.2.2, 00:04:54,
Ethernet0/0
O E2    10.254.0.0/24 [110/50] via 10.5.2.2, 00:04:54,
Ethernet0/0

```

Step 16 Use the **show ip protocols** command to verify the OSPF routing process at the edge and internal routers.

How many areas does the edge router belong to?

How many areas does the internal router belong to?

```

P5R4#show ip protocols
Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router ID 10.200.200.54
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4

```

```

Routing for Networks:
  10.5.0.0 0.0.255.255 area 5
Routing Information Sources:
  Gateway      Distance      Last Update
  200.200.200.200    110      00:00:02
  10.0.0.51          110      00:00:02
  10.200.200.54      110      00:00:02
  10.0.0.52          110      00:00:02
  10.200.200.53      110      00:00:02
  Distance: (default is 110)
P5R1>show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.0.0.51
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.5.0.0 0.0.255.255 area 5
    10.55.0.0 0.0.255.255 area 5
    172.31.5.0 0.0.0.255 area 0
    172.31.55.0 0.0.0.255 area 0
  Routing Information Sources:
  Gateway      Distance      Last Update
  200.200.200.200    110      00:58:23
  100.100.100.100    110      02:43:45
  10.5.3.4            110      20:49:53
  10.5.3.3            110      1d01h
  10.5.2.2            110      1d01h
  10.5.1.1            110      21:39:46
  10.0.0.51           110      00:58:33
  10.200.200.54       110      01:00:37
  10.0.0.52           110      00:58:33
  Gateway      Distance      Last Update
  10.200.200.53       110      00:59:55
  Distance: (default is 110)

```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have configured OSPF over a point-to-multipoint and point-to-point Frame Relay connection.
- You can ping the BBR2 router from your pod.

Lab Exercise 4-4: Understanding the OSPF Database and Tuning OSPF

Complete this lab exercise to practice what you learned in the related lesson.

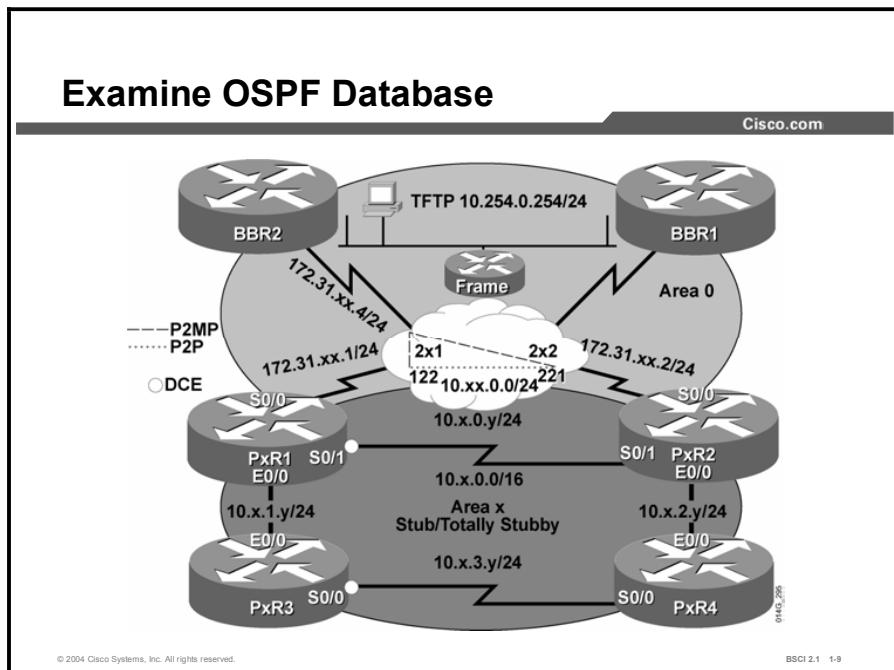
Exercise Objective

In this exercise, you will use **show** commands to view the LSDB structure. You will also investigate the use of OSPF stub areas. After completing this exercise, you will be able to meet these objectives:

- Describe the OSPF LSDB structure
- Describe the available tools necessary to investigate the LSDB
- Limit routing table size and update traffic using OSPF area route summarization
- Limit routing table size and update traffic using the OSPF stub area

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (BBR2) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router)#area x stub	Configures the area to be a stubby area, blocks type 5 LSAs (external routes) from reaching this area, and substitutes a default route to the ABR.
(config-router)#area x stub no-summary	Configures the area to be a totally stubby area, blocks type 3, 4, and 5 LSAs (interarea and external routes) from reaching this area, and substitutes a default route to the ABR.
#show ip ospf database	Shows the LSDB.
#show ip ospf database external	Shows exterior LSAs (LSA type 5).

Job Aids

There are no job aids for this lab exercise.

Task 1: Examining the OSPF Database

In this task you will review the OSPF database and examine all LSAs that are stored in the router.

Exercise Procedure

Complete these steps:

- Step 1** Use the **show ip ospf database** command to display the OSPF database. This database shows all LSAs that are stored in the router. Use Table 3 to interpret the output.

Do you see the LSA types 1, 2, 3, 4, and 5 in the OSPF database?

On the edge routers, do you see LSA information about area 0 and area x ?

On the internal routers, do you see LSA information about area x only?

The following table explains some of the displayed fields.

Table 3: Displayed Fields Information

Field	Information Provided
ADV Router	RID of the advertising router.
Age	Age of the LSA.
Checksum	Checksum of the contents of the LSA.
Link Count	Number of interfaces on the router. Each serial interface counts as two links, and each Ethernet interface counts as one link.
Link ID	A value that uniquely identifies a specific LSA.
Seq#	Sequence number, used to detect an older or duplicate LSA.
Tag	Administratively used to recognize routes that are introduced through a specific redistribution process.

- Step 2** Use the **show ip ospf database external** command to display all the type 5 LSAs in the OSPF database. The core router BBR2 is redistributing the 10.254.0.0/24 network into OSPF. Determine if there is a type 5 LSA for the 10.254.0.0 network. Your display for the edge router should resemble the following:

```
P4R2#show ip ospf database external
OSPF Router with ID (10.0.0.42) (Process ID 1)
Type-5 AS External Link States
    Routing Bit Set on this LSA
    LS age: 577
    Options: (No TOS-capability, DC)
    LS Type: AS External Link
```

```

Link State ID: 10.254.0.0 (External Network Number )
Advertising Router: 200.200.200.200
LS Seq Number: 80000001
Checksum: 0x173F
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 50
Forward Address: 0.0.0.0
External Route Tag: 0

```

Task 2: OSPF Area Route Summarization

In this task, you will identify how to bring the benefits of summarization to OSPF. Summarization reduces the size of routing tables, reduces routing update traffic, and minimizes the impact of flapping lines. In addition, it minimizes processing and memory requirements for all routers.

Exercise Procedure

Complete these steps:

- Step 1** At the edge routers, summarize the pod networks to 10.x.0.0/16 from area *x* using the **area range** command under the OSPF routing process.
- Step 2** From the edge router, Telnet to the BBR2 router (172.31.xx.4) and examine the routing table on BBR2.

Notice that BBR2 recognizes two paths to the pod 10.x.0.0/16 network. It no longer recognizes each of the pod /24 links (10.x.0.0/24, 10.x.1.0/24, 10.x.2.0/24, and 10.x.3.0/24).

BBR2 still recognizes the 10.xx.0.0/24 link because it is not part of the summarized range.

Your display should resemble the following:

```

BBR2#show ip route
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
      inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
      type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E
      - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
      IS-IS inter area
      * - candidate default, U - per-user static route, o -
      ODR
      P - periodic downloaded static route

```

Gateway of last resort is not set

```
172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
C      172.31.55.0/24 is directly connected, Serial0/0.5
O      172.31.33.2/32 [110/781] via 172.31.33.2, 00:25:14,
Serial0/0.3
C      172.31.33.0/24 is directly connected, Serial0/0.3
O      172.31.33.1/32 [110/781] via 172.31.33.1, 00:25:14,
Serial0/0.3
C      172.31.44.0/24 is directly connected, Serial0/0.4
C      172.31.22.0/24 is directly connected, Serial0/0.2
C      172.31.66.0/24 is directly connected, Serial0/0.6
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O IA   10.3.0.0/16 [110/791] via 172.31.33.1, 00:00:33,
Serial0/0.3
                                         [110/791] via 172.31.33.2, 00:00:33,
Serial0/0.3
O IA   10.33.0.0/24 [110/1562] via 172.31.33.2, 00:25:14,
Serial0/0.3
                                         [110/1562] via 172.31.33.1, 00:25:14,
Serial0/0.3
C      10.254.0.0/24 is directly connected, Ethernet0/0
```

Step 3 Determine the changes that summarization made to the routing table on the edge routers. Is the routing table reduced on the edge routers? Explain why there is a route to Null0. Your display should resemble the following:

```
P3R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.31.55.4/32 [110/781] via 172.31.33.4, 00:03:09,
Serial0/0.1
```

```

C      172.31.33.0/24 is directly connected, Serial0/0.1
O      172.31.33.1/32 [110/1562] via 172.31.33.4, 00:03:09,
Serial0/0.1
O      172.31.33.4/32 [110/781] via 172.31.33.4, 00:03:09,
Serial0/0.1
O      172.31.44.4/32 [110/781] via 172.31.33.4, 00:03:09,
Serial0/0.1
O      172.31.22.4/32 [110/781] via 172.31.33.4, 00:03:09,
Serial0/0.1
O      172.31.66.4/32 [110/781] via 172.31.33.4, 00:03:10,
Serial0/0.1
          10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O      10.3.1.0/24 [110/791] via 10.3.0.1, 00:03:10,
Serial0/1
O      10.3.0.0/16 is a summary, 00:03:10, Null0
C      10.3.0.0/24 is directly connected, Serial0/1
O      10.3.3.0/24 [110/791] via 10.3.2.4, 00:03:10,
Ethernet0/0
C      10.3.2.0/24 is directly connected, Ethernet0/0
C      10.33.0.0/24 is directly connected, Serial0/0.2
O E2    10.254.0.0/24 [110/50] via 172.31.33.4, 00:03:11,
Serial0/0.1

```

Step 4 Configure the pod OSPF area as a stub area (remember to configure both the edge and internal routers, because the stub flag is included in hellos). Notice the error messages and that no adjacency is established until both routers agree that they are stubs. What changes do you expect to occur with the implementation of a stub?

Step 5 Examine the edge (PxR1 or PxR2) and internal (PxR3 or PxR4) routing tables.

Determine if there are any interarea OSPF routes in the internal routers and the reason for their presence.

Notice that the internal routers do not have any external routes. The ABR (edge router) generates a default route to the internal routers for reaching external networks. Your display should resemble the following:

```

P3R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR

```

P - periodic downloaded static route

Gateway of last resort is not set

```
    172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.31.55.4/32 [110/781] via 172.31.33.4, 00:01:46,
Serial0/0.1
O      172.31.33.2/32 [110/1562] via 172.31.33.4, 00:01:46,
Serial0/0.1
C      172.31.33.0/24 is directly connected, Serial0/0.1
O      172.31.33.4/32 [110/781] via 172.31.33.4, 00:01:46,
Serial0/0.1
O      172.31.44.4/32 [110/781] via 172.31.33.4, 00:01:46,
Serial0/0.1
O      172.31.22.4/32 [110/781] via 172.31.33.4, 00:01:46,
Serial0/0.1
O      172.31.66.4/32 [110/781] via 172.31.33.4, 00:01:47,
Serial0/0.1
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C      10.3.1.0/24 is directly connected, Ethernet0/0
O      10.3.0.0/16 is a summary, 00:01:03, Null0
C      10.3.0.0/24 is directly connected, Serial0/1
O      10.3.3.0/24 [110/791] via 10.3.1.3, 00:01:03,
Ethernet0/0
O      10.3.2.0/24 [110/791] via 10.3.0.2, 00:01:04,
Serial0/1
C      10.33.0.0/24 is directly connected, Serial0/0.2
O E2    10.254.0.0/24 [110/50] via 172.31.33.4, 00:01:04,
Serial0/0.1
```

P3R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

```

Gateway of last resort is 10.3.1.1 to network 0.0.0.0

    172.31.0.0/32 is subnetted, 7 subnets
O IA      172.31.55.4 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
O IA      172.31.33.2 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
                                [110/791] via 10.3.3.4, 00:00:47,
Serial0/0
O IA      172.31.33.1 [110/10] via 10.3.1.1, 00:00:47,
Ethernet0/0
O IA      172.31.33.4 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
O IA      172.31.44.4 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
O IA      172.31.22.4 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
O IA      172.31.66.4 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
          10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C         10.3.1.0/24 is directly connected, Ethernet0/0
O         10.3.0.0/24 [110/791] via 10.3.1.1, 00:00:47,
Ethernet0/0
C         10.3.3.0/24 is directly connected, Serial0/0
O         10.3.2.0/24 [110/791] via 10.3.3.4, 00:00:50,
Serial0/0
O IA      10.33.0.0/24 [110/791] via 10.3.1.1, 00:00:50,
Ethernet0/0
C         10.200.200.33/32 is directly connected, Loopback0
O*IA   0.0.0.0/0 [110/11] via 10.3.1.1, 00:00:50, Ethernet0/0

```

Step 6 Configure the OSPF area of the pod as totally stubby. Remember that only the ABR requires the command to configure the area as totally stubby.

Step 7 Ping the TFTP server to verify connectivity.

Step 8 Examine the edge (PxR1 or PxR2) and internal (PxR3 or PxR4) routing tables.

Determine if there are any interarea OSPF routes in the internal routers and the reason for their presence. Your display should resemble the following:

```

P3R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP

```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -  
IS-IS inter area  
* - candidate default, U - per-user static route, o -  
ODR  
P - periodic downloaded static route
```

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

```
    172.31.0.0/16 is variably subnetted, 7 subnets, 2 masks  
O      172.31.55.4/32 [110/781] via 172.31.33.4, 00:00:21,  
Serial0/0.1  
O      172.31.33.2/32 [110/1562] via 172.31.33.4, 00:00:21,  
Serial0/0.1  
C      172.31.33.0/24 is directly connected, Serial0/0.1  
O      172.31.33.4/32 [110/781] via 172.31.33.4, 00:00:21,  
Serial0/0.1  
O      172.31.44.4/32 [110/781] via 172.31.33.4, 00:00:21,  
Serial0/0.1  
O      172.31.22.4/32 [110/781] via 172.31.33.4, 00:00:21,  
Serial0/0.1  
O      172.31.66.4/32 [110/781] via 172.31.33.4, 00:00:22,  
Serial0/0.1  
          10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks  
C      10.3.1.0/24 is directly connected, Ethernet0/0  
O      10.3.0.0/16 is a summary, 00:00:02, Null0  
C      10.3.0.0/24 is directly connected, Serial0/1  
O      10.3.3.0/24 [110/791] via 10.3.1.3, 00:00:02,  
Ethernet0/0  
O      10.3.2.0/24 [110/801] via 10.3.1.3, 00:00:04,  
Ethernet0/0  
C      10.33.0.0/24 is directly connected, Serial0/0.2  
O E2    10.254.0.0/24 [110/50] via 172.31.33.4, 00:00:04,  
Serial0/0.1
```

```
P3R3>show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M -  
mobile, B - BGP
```

```
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF  
inter area
```

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external  
type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2, E  
- EGP
```

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -  
IS-IS inter area
```

```

* - candidate default, U - per-user static route, o -
ODR

P - periodic downloaded static route

Gateway of last resort is 10.3.1.1 to network 0.0.0.0
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.3.1.0/24 is directly connected, Ethernet0/0
O        10.3.0.0/24 [110/791] via 10.3.1.1, 00:00:55,
Ethernet0/0
C        10.3.3.0/24 is directly connected, Serial0/0
O        10.3.2.0/24 [110/791] via 10.3.3.4, 00:00:55,
Serial0/0
C        10.200.200.33/32 is directly connected, Loopback0
O*IA 0.0.0.0/0 [110/11] via 10.3.1.1, 00:00:55, Ethernet0/0

```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have examined the OSPF database and can describe the tools necessary to investigate the LSDB.
- You have configured your pod router area as an OSPF stub area and as a totally stubby area.
- You have minimized routing table size by using route summarization without affecting reachability—you should still be able to ping all devices in your pod and in the core.

Lab Exercise 4-5: Configuring OSPF Virtual Links (Optional)

Complete this lab exercise to practice what you learned in the related lesson.

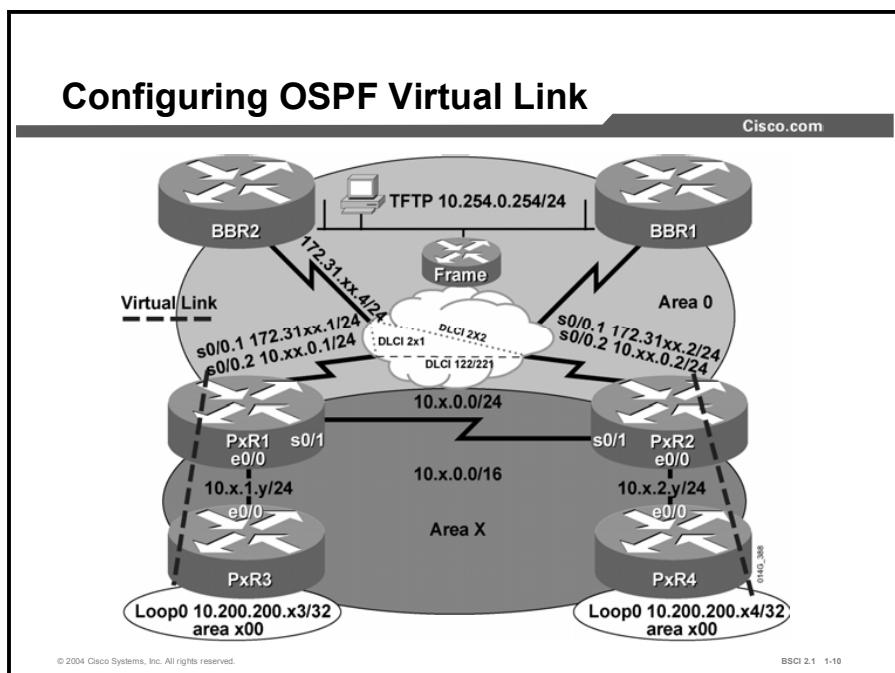
Exercise Objective

In this exercise, you will investigate OSPF virtual links. After completing this exercise, you will be able to meet these objectives:

- Use virtual links to connect an area to area 0

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (BBR2) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4 and connected to a central core. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router) #area x virtual-link 10.0.0.xy	Creates a virtual link. The area number is the transit area. The IP address is the RID of the far end.
#show ip ospf	Shows information about the OSPF process on the router, including all areas that are connected to the router.
#show ip ospf neighbor	Shows a list of OSPF neighbors, and their RID.
#show ip ospf virtual-links	Shows the status of virtual links.
#show ip route	Shows the forwarding table of the router.

Job Aids

There are no job aids for this lab exercise.

Task 1: Configuring the OSPF Virtual Link

OSPF requires that all areas have a connection to area 0, the backbone. In this lab, you will create a discontiguous area and examine the resulting routing tables. You will then configure a virtual link that connects the new area to area 0.

Exercise Procedure

Complete these steps:

- Step 1** Remove the OSPF stub configuration from all the pod routers.
- Step 2** On the internal routers, PxR3 and PxR4, shut down the serial 0/0 interface, disconnecting the link between them.
- Step 3** Place the loopback interface on each internal router into a new OSPF area, using area number $x00$, where x is your pod number. This requires an additional network statement under the OSPF router configuration.
- Step 4** Examine the routing table on the edge routers, PxR1 and PxR2. Is the network for the loopback interface of the internal router (10.200.200.xy) present in the routing table?
- Step 5** Because OSPF assumes that all areas will have at least one interface in area 0, the internal routers will not advertise the loopback interface to the edge routers. However, area $x00$ does not border area 0.

You will remedy this situation by configuring a virtual link from area $x00$ to area 0. As the first step in configuring the virtual link, discover the RID of each router. Your display should resemble the following:

```
P5R1#show ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface
10.200.200.53    1     FULL/DR        00:00:38      10.5.1.3
Ethernet0/0
200.200.200.200  1     FULL/ -        00:01:45      172.31.55.4
Serial0/0.1
```

```
P5R3#show ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface
10.0.0.51        1     FULL/BDR       00:00:34      10.5.1.1
Ethernet0/0
```

- Step 6** Configure an OSPF virtual link from the internal router to the edge router, through area x , where x is your pod number.

- Step 7** Verify that the virtual link is functioning. Your display should resemble the following:

```
P5R3#show ip ospf virtual-links
Virtual Link OSPF_VL0 to router 10.0.0.51 is up
    Run as demand circuit
    DoNotAge LSA allowed.
    Transit area 5, via interface Ethernet0/0, Cost of using 10
    Transmit Delay is 1 sec, State POINT_TO_POINT,
    Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Retransmit 5
        Hello due in 00:00:05
        Adjacency State FULL (Hello suppressed)
        Index 1/2, retransmission queue length 0, number of
        retransmission 1
        First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
        Last retransmission scan length is 1, maximum is 1
        Last retransmission scan time is 0 msec, maximum is 0 msec
```

- Step 8** Verify that the network for the loopback interface of the internal router now appears in the routing table of the edge router.

- Step 9** On the internal router, issue the **show ip ospf** command. Which OSPF areas are active on this router?

OSPF treats the virtual link as if it were an interface belonging to area 0. Thus, you will see three areas active on the router: area x, area x00, and area 0.

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have used virtual links to heal a discontiguous area
- You have used virtual links to create an arbitrary topology of areas

Lab Exercise 5-1: Configuring Integrated IS-IS in Multiple Areas

Complete this lab exercise to practice what you learned in the related lesson.

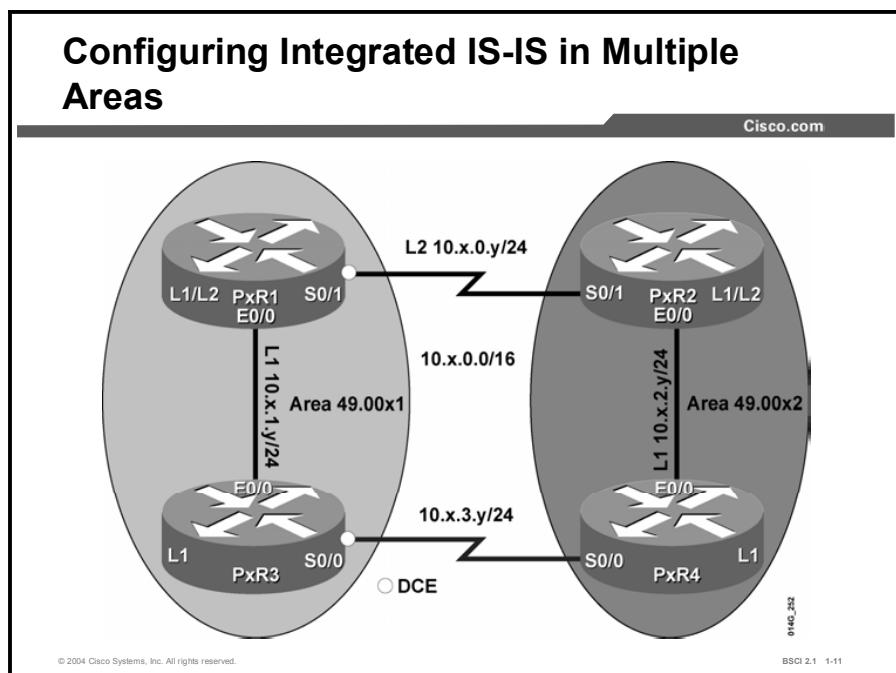
Exercise Objective

In this exercise, you will configure your pod for IS-IS routing. After completing this exercise, you will be able to meet these objectives:

- Connect to other devices using IS-IS routes

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4). These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers

This lab exercise requires a topology of a pod. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config)#router isis	Turns on IS-IS.
(config-if)#isis circuit level-2 only	Sets this interface to participate in only Level 2 routing.
(config-router)#is-type level-1	Sets this router to participate in only Level 1 routing.
(config-router)#net 49.0031.3333.3333.3333.00	Identifies the NET to be used for this device—CLNS addresses identify a device, not an interface.
(config-router)#summary-address 10.3.2.0 255.255.254.0 level-2	Creates a summary route into Level 2.
Config-if)#ip router isis	Enables IS-IS routing on an interface.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up and Preparing

In this task you will remove all OSPF configurations in order to configure your pod for IS-IS routing.

Exercise Procedure

Complete these steps:

- Step 1** Remove all OSPF configurations from the internal routers (PxR3 and PxR4.) Verify that interface s0/0 is enabled on these routers. If the interface is shut, no shut it.
- Step 2** Remove all OSPF configurations from the edge routers. Remember to remove the **ip ospf network point-to-multipoint** command on the s0/0.1 subinterface.
- Step 3** Shut down the serial 0/0 interface on the edge routers (PxR1 and PxR2) to isolate your pod from the core for this lab. No shut the serial s0/1 interface between these two routers.

Task 2: Configuring Integrated IS-IS in Multiple Areas

In this task you will be configuring IS-IS in multiple areas.

Exercise Procedure

Complete these steps:

- Step 1** Configure IS-IS on the pod routers. PxR1 and PxR3 should be in area 49.00x1. PxR2 and PxR4 should be in area 49.00x2. Assign a NET to each router as shown in the table here.

Router	NET	Example (Pod 7)
PxR1	49.00x1.yyyy.yyyy.yyyy.00	49.0071.1111.1111.1111.00
PxR2	49.00x2. yyyy.yyyy.yyyy.00	49.0072.2222.2222.2222.00
PxR3	49.00x1.yyyy.yyyy.yyyy.00	49.0071.3333.3333.3333.00
PxR4	49.00x2. yyyy.yyyy.yyyy.00	49.0072.4444.4444.4444.00

- Step 2** Enable IS-IS on the active serial, loopback, and Ethernet interfaces of all the routers within your pod using the **ip router isis** command.
- Step 3** Leave the edge routers as the default IS type of L1/L2; however, set up internal routers to participate only in Level 1 using the proper IS-IS router configuration command. When the setup is complete, all communication between the areas will go through the edge routers.

- Step 4** All routers are L1/L2 by default. Level 1 communication takes place only if the areas match, however, so PxR3 and PxR4 will not form a Level 1 adjacency with each other because they are in different areas. They will form an adjacency only with their directly connected edge router. PxR1 and PxR2 will form a Level 2 communication.

Look at the IS-IS topology for an internal router and note that the internal router should have a Level 1 adjacency with the edge router. Trace the path from one internal router to the loopback address of the opposite internal router. The trace should show that the path to reach the opposite internal router loopback goes through the edge router.

Your display should resemble the following:

```
P3R3#sh isis topology
IS-IS paths to level-1 routers
System Id          Metric  Next-Hop           Interface
SNPA
P3R1                10      P3R1               Et0/0
0008.e3e7.e600

P3R3                --
P3R3#trace 10.200.200.34
Type escape sequence to abort.
Tracing the route to 10.200.200.34
  1 10.3.1.1 4 msec 4 msec 0 msec
  2 10.3.0.2 16 msec 12 msec 16 msec
  3 10.3.2.4 16 msec * 12 msec
P3R3#
```

- Step 5** Look at the routing table on the internal routers. Notice that IS-IS Level 1 routing tables resemble OSPF totally stubby areas. For instance, where is the route to the loopback address that you just pinged?

Your display should resemble the following:

```
P3R3#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
Gateway of last resort is 10.3.1.1 to network 0.0.0.0
```

```

        10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C      10.3.1.0/24 is directly connected, Ethernet0/0
i L1   10.3.0.0/24 [115/20] via 10.3.1.1, Ethernet0/0
C      10.3.3.0/24 is directly connected, Serial0/0
C      10.200.200.33/32 is directly connected, Loopback0
i*L1  0.0.0.0/0 [115/10] via 10.3.1.1, Ethernet0/0
P3R3#

```

- Step 6** Take a look at the IS-IS topology table on the edge routers. Although these routers participate in Level 1 and Level 2 routing, they are using only Level 1 on the Ethernet interface and only Level 2 on the serial interface.

Your display should resemble the following:

```

P3R2#sh isis topology
IS-IS paths to level-1 routers
System Id          Metric  Next-Hop           Interface
SNPA
P3R2                --      P3R4               Et0/0
P3R4      10      P3R4
0008.e3e7.fd60

IS-IS paths to level-2 routers
System Id          Metric  Next-Hop           Interface
SNPA
P3R1      10      P3R1               Se0/1
*HDLC*
P3R2                --      P3R3
P3R3                **      P3R4
P3R4                **
P3R2#

```

- Step 7** Use the proper IS-IS interface configuration command to remove the redundant but unused hellos by forcing PxR1 and PxR2 to participate in a single routing level on each interface (Ethernet = Level 1 only, and Serial = Level 2 only).

Redundancy (forming both Level 1 and Level 2 adjacencies) wastes bandwidth and router resources.

- Step 8** On PxR1, summarize the 10.x.0.0 and the 10.x.1.0 networks to 10.x.0.0/23. On PxR2, summarize the 10.x.2.0/24 and the 10.x.3.0/24 networks to 10.x.2.0/23. Examine the routing tables on PxR1 and PxR2 to verify that the summary route appears.

Your display should resemble the following:

```

P5R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area

```

```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
    IS-IS inter area
    * - candidate default, U - per-user static route, o -
    ODR
    P - periodic downloaded static route

```

Gateway of last resort is not set

```

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
i L1      10.5.3.0/24 [115/20] via 10.5.1.3, Ethernet0/0
i L2      10.5.2.0/23 [115/20] via 10.5.0.2, Serial0/1
C         10.5.1.0/24 is directly connected, Ethernet0/0
i su     10.5.0.0/23 [115/10] via 0.0.0.0, Null0
C         10.5.0.0/24 is directly connected, Serial0/1
P5R1#

```

```

p5r2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
    inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
    type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2, E
    - EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
    IS-IS inter area
    * - candidate default, U - per-user static route, o -
    ODR
    P - periodic downloaded static route

```

Gateway of last resort is not set

```

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
i L1      10.5.3.0/24 [115/20] via 10.5.2.4, Ethernet0/0
i su     10.5.2.0/23 [115/10] via 0.0.0.0, Null0
C         10.5.2.0/24 is directly connected, Ethernet0/0
i L2      10.5.0.0/23 [115/20] via 10.5.0.1, Serial0/1
C         10.5.0.0/24 is directly connected, Serial0/1
p5r2#

```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- IS-IS is configured properly and exchanging routes.
- IS-IS has been optimized to use only one type of hello over each link.
- IS-IS has been optimized to pass a summary route.

Lab Exercise 6-1: Configuring Basic Redistribution

Complete this lab exercise to practice what you learned in the related lesson.

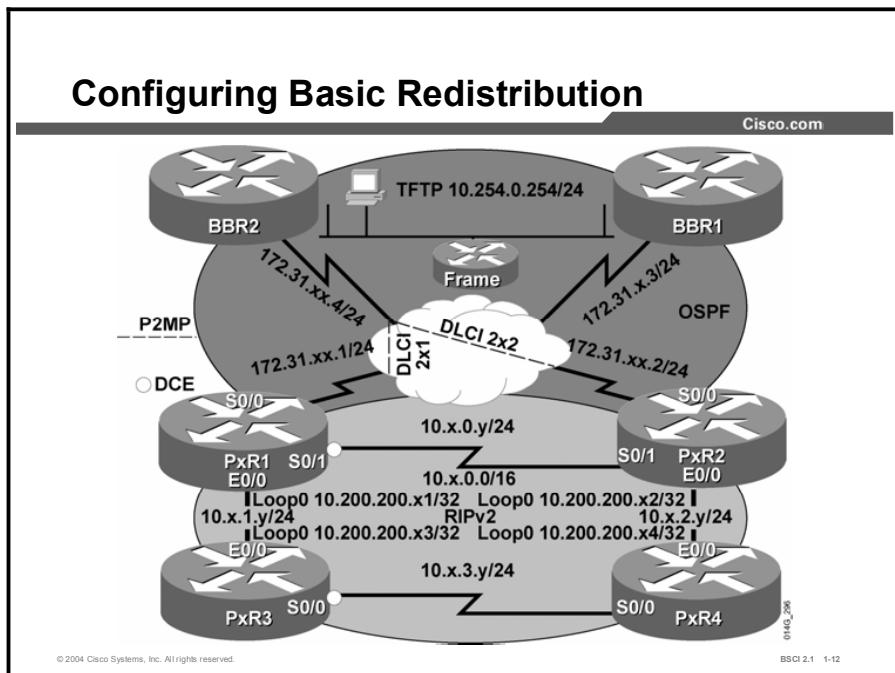
Exercise Objective

In this exercise, you will redistribute routes from RIPv2 into OSPF and supply a default route to the RIPv2 routing domain. After completing this exercise, you will be able to meet this objective:

- Redistribute routing information between different protocols

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this lab exercise. Your instructor will assign you to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router) #default-information originate	Advertises the default route through RIP.
(config)#ip route 0.0.0.0 0.0.0.0 172.31.xx.4	Creates a static default route.
(config-router) #no auto-summary	Does not automatically summarize routes at classful boundaries.
(config-router) # redistribute rip subnets	Redistributes RIPv2 into OSPF. The subnets keyword enables the passing of subnetted routes into OSPF.
(config-router) #version 2	Runs RIPv2.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

The quickest way to begin to investigate redistribution is to remove the IS-IS configuration. However, you may also copy the setup file of the router (PxRy.txt) to startup-config, and reload, and then supply the **ip classless** command.

Exercise Procedure

Complete these steps:

- Step 1** Remove the IS-IS configuration from all the pod routers using the **no router isis** global configuration command.
- Step 2** Create a loopback interface on each router with the IP address of 10.200.200.xy /32, where x is the pod number and y is the router number. This address may already be on your internal routers.
- Step 3** Check the configuration of s0/0 on the edge routers. It should include an IP address, Frame Relay encapsulation, and Frame Relay static map, and have Frame Relay Inverse Address Resolution Protocol (ARP) turned off.

The IP address should be 172.31.xx.y /24 and the Data Link Connection Identifier (DLCI) should be 2xy, where x is the pod number and y is the router number.

You may have to delete the current configuration and configure the proper settings. The easiest way to do this is with the **default interface s0/0** command.

Your s0/0 interface on the edge routers should resemble following:

```
interface Serial0/0
  ip address 172.31.33.1 255.255.255.0
  encapsulation frame-relay
  frame-relay map ip 172.31.33.4 231 broadcast
  no frame-relay inverse-arp
```

Note	You will need to configure the Frame Relay configurations on your s0/0 interface if you copied the startup file and reloaded your router or used default interface s0/0.
-------------	--

Task 2: Setting up Routing Protocols

In this task, you will set up the routing protocols in order to configure basic redistribution. The instructor has placed BBR2 in OSPF area 0.

Exercise Procedure

Complete these steps:

Step 1 The instructor has placed BBR2 in OSPF area 0.

Configure the edge and internal routers as follows:

The edge routers of each pod run both OSPF and RIPv2.

On the edge routers, place serial 0/0 in OSPF area 0.

Because BBR2 is configured with a point-to-multipoint interface, configure the s0/0 interface of the edge router with the OSPF point-to-multipoint network type.

The internal routers run only RIPv2.

Your display should resemble the following:

On the edge routers:

```
P3R1(config)#router ospf 1
P3R1(config-router)#network 172.31.33.0 0.0.0.255 area 0
P3R1(config-router)#router rip
P3R1(config-router)#version 2
P3R1(config-router)#network 10.0.0.0
P3R1(config-router)#no auto-summary
P3R1(config-router)#end
P3R1(config)#int s0/0
P3R1(config-if)#ip ospf network point-to-multipoint
P3R1(config-if)#end
```

On the interior routers:

```
P3R3(config)#router rip
P3R3(config-router)#network 10.0.0.0

P3R3(config-router)#version 2
P3R3(config-router)#end
```

Step 2 Show the IP routing table on both edge routers. Verify that both edge routers are learning both OSPF and RIPv2 routes.

On the RIPv2 routes to the networks within your pod, what is the highest RIP hop count?

Task 3: Configuring Basic Redistribution

In this task, you will configure basic redistribution from RIPv2 into OSPF.

Exercise Procedure

Complete these steps:

- Step 1** Configure both edge routers to pass a default route into RIPv2. Remember that the RIPv2 router needs a static default route configured in order to advertise it to other RIPv2 routers.

Examine the routing table on the internal routers.

Is the default route present?

What is its path and metric?

- Step 2** Configure both edge routers to redistribute RIPv2 routes into OSPF without specifying a metric value.

What will be the default metric that is used by OSPF when the RIPv2 routes are redistributed?

It is important for you to remember to include the **subnets** keyword in the redistribution statement.

- Step 3** Telnet to the core router BBR2 and examine the OSPF database.

Which routes in the routing table were redistributed from your pod?

What type of OSPF routes are they?

- Step 4** Examine the IP routing table on both internal routers. Your display should resemble the following:

```
P3R4#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route

Gateway of last resort is 10.3.3.3 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
```

```

R      10.3.0.0/24 [120/1] via 10.3.2.2, 00:00:03, Ethernet0/0
R      10.3.1.0/24 [120/1] via 10.3.3.3, 00:00:01, Serial0/0
C      10.3.3.0/24 is directly connected, Serial0/0
C      10.3.2.0/24 is directly connected, Ethernet0/0
R      10.200.200.31/32 [120/2] via 10.3.3.3, 00:00:01,
Serial0/0
C      10.200.200.34/32 is directly connected, Loopback0
R      10.200.200.32/32 [120/1] via 10.3.2.2, 00:00:03,
Ethernet0/0
R      10.200.200.33/32 [120/1] via 10.3.3.3, 00:00:01,
Serial0/0
R*    0.0.0.0/0 [120/2] via 10.3.3.3, 00:00:02, Serial0/0

```

Task 4: Filtering Routing Updates

Configure your edge routers to filter information about the loopback addresses to the core. Because the core is exchanging OSPF routes with your pod, use a distribute list to block these routes from being redistributed into OSPF.

Exercise Procedure

Complete these steps:

- Step 1** Create an access list that will match the four loopback addresses.
- Step 2** Use a distribute list to block the RIPv2 routes in this access list from being redistributed into OSPF.
- Step 3** Examine the routing table on the core. Verify that the loopback addresses are not listed.
- Step 4** Can the core ping your loopback addresses?

Exercise Verification

You have completed this exercise when you attain these results:

- You can establish OSPF adjacencies between the edge routers and the core BBR2 router, and exchange the routing updates.
- You can establish that the RIPv2 updates are exchanged between the internal routers and the edge routers.
- You can establish that redistribution is configured from RIPv2 to OSPF.
- You can demonstrate that a default route has been injected into the RIPv2 routing domain.

Lab Exercise 6-2: Tuning Basic Redistribution with Cisco IOS Tools

Complete this lab exercise to practice what you learned in the related lesson.

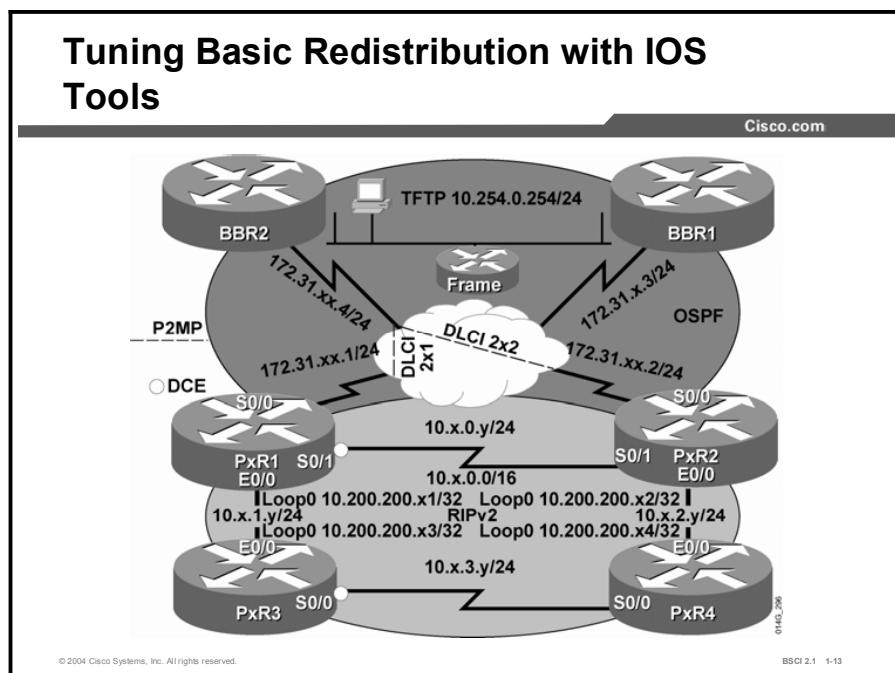
Exercise Objective

In this exercise, you will configure a route map to control redistribution. After completing this exercise, you will be able to meet this objective:

- Use a route map to translate metrics from RIP to OSPF to aid in redistribution

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core (BBR2) through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-route-map) # match metric 1	Matches source protocol metric.
(config-route-map) # set metric 1000	Sets destination protocol metric.
(config-router) # redistribute rip subnets route-map CONVERT	Redistributes using the route map.
(config) #route-map CONVERT permit 10	Creates a route map statement.

Job Aids

There are no job aids for this lab exercise.

Task 1: Tuning Basic Redistribution with Route Maps

In this task you will use route maps to tune the basic redistribution configuration.

Exercise Procedure

Complete these steps:

- Step 1** Telnet to BBR2. Notice that all of your pod routes (10.x.0.0) have the same OSPF metric of 20. Your display should resemble the following. Note that the exact routes will depend on the pods being used.

```
P3R2#172.31.33.4
Trying 172.31.33.4 ... Open

BBR2#sh ip route
(output omitted)
Gateway of last resort is not set

    172.31.0.0/16 is variably subnetted, 14 subnets, 2 masks
C      172.31.55.0/24 is directly connected, Serial0/0.5
O      172.31.33.2/32 [110/781] via 172.31.33.2, 00:23:08,
Serial0/0.3
C      172.31.33.0/24 is directly connected, Serial0/0.3
O      172.31.33.1/32 [110/781] via 172.31.33.1, 00:23:08,
Serial0/0.3
C      172.31.44.0/24 is directly connected, Serial0/0.4
C      172.31.22.0/24 is directly connected, Serial0/0.2
C      172.31.11.0/24 is directly connected, Serial0/0.1
C      172.31.66.0/24 is directly connected, Serial0/0.6
    10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
O E2    10.3.1.0/24 [110/20] via 172.31.33.1, 00:10:50,
Serial0/0.3
O E2    10.3.3.0/24 [110/20] via 172.31.33.2, 00:02:12,
Serial0/0.3
O E2    10.3.2.0/24 [110/20] via 172.31.33.2, 00:10:48,
Serial0/0.3
C      10.254.0.0/24 is directly connected, Ethernet0/0
```

Step 2 Having the same metric for all the redistributed RIP routes prevents the core from making accurate routing decisions for those routes. The central OSPF domain needs to have different OSPF metrics based on how far away the network is from the redistribution point.

At the edge routers, create a route map for altering the metric of the redistributed routes. Match the RIP metric and set an appropriate OSPF metric, as in this example:

Match RIP hop count of 1, set OSPF metric to 1000.

Match RIP hop count of 2, set OSPF metric to 2000.

Step 3 At the edge routers, change the redistribution from RIP to OSPF to use this route map.

Step 4 View the routing table on BBR2. Has it converted the metrics appropriately? Your display should resemble the following:

```
BBR2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
          * - candidate default, U - per-user static route, o -
ODR
          P - periodic downloaded static route
```

Gateway of last resort is not set

```
      172.31.0.0/16 is variably subnetted, 14 subnets, 2 masks
C        172.31.55.0/24 is directly connected, Serial0/0.5
O        172.31.33.2/32 [110/781] via 172.31.33.2, 00:31:58,
Serial0/0.3
C        172.31.33.0/24 is directly connected, Serial0/0.3
O        172.31.33.1/32 [110/781] via 172.31.33.1, 00:31:58,
Serial0/0.3
C        172.31.44.0/24 is directly connected, Serial0/0.4
C        172.31.22.0/24 is directly connected, Serial0/0.2
C        172.31.11.0/24 is directly connected, Serial0/0.1
C        172.31.66.0/24 is directly connected, Serial0/0.6
      10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
```

```
O E2      10.3.1.0/24 [110/2000] via 172.31.33.2, 00:02:21,  
Serial0/0.3  
O E2      10.3.3.0/24 [110/1000] via 172.31.33.1, 00:02:45,  
Serial0/0.3  
O E2      10.3.2.0/24 [110/2000] via 172.31.33.1, 00:02:45,  
Serial0/0.3  
C        10.254.0.0/24 is directly connected, Ethernet0/0
```

Exercise Verification

You have completed this exercise when you attain this result:

- You can demonstrate how to use a route map to control redistribution.

Lab Exercise 6-3: Configuring Policy-Based Routing (Optional)

Complete this lab exercise to practice what you learned in the related lesson.

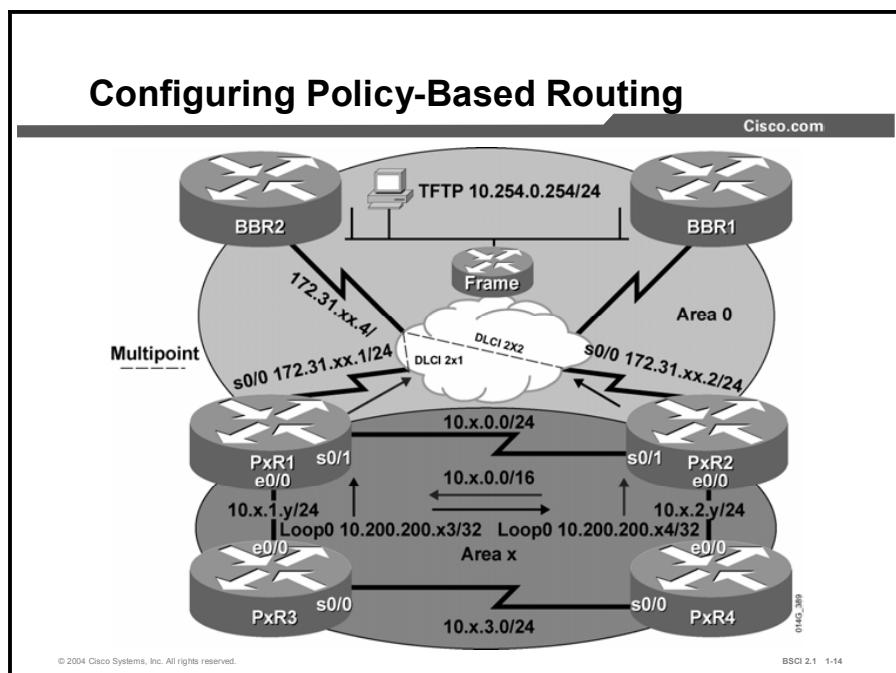
Exercise Objective

In this exercise, you will use PBR to exert the maximum administrative control over how traffic is handled. After completing this exercise, you will be able to meet this objective:

- Configure PBR

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config)#access-list 2 permit 10.200.200.0 0.0.0.255	Creates an access list for use with policy routing.
(config-route-map)#match ip address 2	Links the access list to the route map, to identify traffic to be policy-routed.
(config-if)#ip policy route-map PBR	Uses this route map on this interface for PBR.
(config)#route-map PBR permit 10	Creates a route map for use with policy routing.
(config-route-map)#set interface s0/1	Alternative to set ip next-hop command. Policy-routes traffic matching access list 2 out interface s0/1.
(config-route-map)#set ip next- hop 10.x.0.2	Uses the listed IP address as the next hop for traffic matching access list 2.

Job Aids

There are no job aids for this lab exercise.

Task 1: Configure PBR

The goal of this lab is to show that PBR can be used to set an arbitrary path, rather than relying on the normal path selection of the router. For the purposes of this lab, suppose you want to control the path that is taken by traffic that is sourced from the loopback interface of the internal router (PxR3 or PxR4).

Normally, traffic from the loopback interface of PxR3, bound out of the pod, would go to PxR1, and then to the backbone router. Similarly, traffic from the loopback of PxR4, bound out of the pod, would go to PxR2 and then to the backbone.

In this lab, you will force traffic from the loopback interface on PxR3 to go through PxR1, then to PxR2, then to the backbone router. Traffic that is sourced from the loopback interface of PxR4 will be forced to go through PxR2, then to PxR1, then to the backbone router.

Exercise Procedure

Complete these steps:

- Step 1** Remove the distribute list from the OSPF router configuration. Otherwise, BBR2 will not have a route to your loopback interfaces.
- Step 2** On both the edge routers, create an access list 2 to match the loopback address on the directly connected internal router.
- Step 3** On the edge routers, PxR1 and PxR2, create a route map. Match the source address of the loopback0 of the internal router by referencing the access list created in Step 1.

Set the outbound interface so that this traffic will be sent out interface serial 0/1, over to the other edge router. Thus, traffic that is sourced from the loopback interface of the internal router will be forced to go to the other edge router before going out to the core router.

What will happen to traffic that is sourced from IP addresses that are not listed in the access list?

- Step 4** Recall that policies are applied on the interface where that traffic enters the router. What is the incoming interface for traffic from the internal router? Apply the policy to that interface.
- Step 5** Verify that the policy is in place and applied to the correct interface, with the **show ip policy** command.

- Step 6** Go to the internal routers and use traceroute to test the policy. First, trace from the internal router to BBR2 (172.31.xx.4). Your display should resemble the following. The trace packet will be sourced from the e0/0 interface of the internal router by default, so it will be routed normally to the BBR2 router.

```
P3R4#trace 172.31.33.4

Type escape sequence to abort.
Tracing the route to 10.254.0.2

1 10.3.2.2 4 msec 4 msec 0 msec
2 172.31.33.4 28 msec * 44 msec
```

Step 7 Next, use extended traceroute, sourced from loopback0, from the internal router to BBR2 (172.31.xx.4). Your display should resemble the following. Because the trace packet is sourced from the loopback interface of the internal router, it will be policy-routed via the other edge router to the BBR2 router.

```
P3R3#trace

Protocol [ip]:
Target IP address: 172.31.33.4
Source address: 10.200.200.33
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none] :
Type escape sequence to abort.
Tracing the route to 10.254.0.2

1 10.3.1.1 52 msec 4 msec 28 msec
2 10.3.0.2 28 msec 24 msec 28 msec
3 172.31.33.4 24 msec * 68 msec
```

- Step 8** View the configured route map to see what traffic has been policy-routed. Your output should resemble the following:

```
P3R1#show route-map

route-map PBR, permit, sequence 10
Match clauses:
    ip address (access-lists): 2
Set clauses:
    interface Serial 0/1
Policy routing matches: 5 packets, 300 bytes
```

- Step 9** On the edge router, turn on debugging of the policy routing. Then go to the internal router and repeat the traceroutes from the internal router to BBR2. You will see the router making the choice to policy-route or not. Your output should resemble the following (some output has been omitted because of length):

```
P5R1#debug ip policy  
1w5d: IP: s=10.5.1.3 (Ethernet0/0), d=172.31.55.4  
(Serial0/0.2), len 100, policy rejected -- normal forwarding  
1w5d: IP: s=10.5.1.3 (Ethernet0/0), d=172.31.55.4  
(Serial0/0.2), len 100, policy rejected -- normal forwarding  
1w5d: IP: s=10.5.1.3 (Ethernet0/0), d=172.31.55.4  
(Serial0/0.2), len 100, policy rejected -- normal forwarding  
1w5d: IP: s=10.5.1.3 (Ethernet0/0), d=172.31.55.4  
(Serial0/0.2), len 100, policy rejected -- normal forwarding  
1w5d: IP: s=10.200.200.53 (Ethernet0/0), d=172.31.55.4, len  
28, policy match  
1w5d: IP: route map PBR, item 10, permit  
1w5d: IP: s=10.200.200.53 (Ethernet0/0), d=172.31.55.4  
(Serial0/1), len 28, policy routed  
1w5d: IP: Ethernet0/0 to Serial0/1 172.31.55.4  
1w5d: IP: s=10.200.200.53 (Ethernet0/0), d=172.31.55.4, len  
28, policy match  
1w5d: IP: route map PBR, item 10, permit  
1w5d: IP: s=10.200.200.53 (Ethernet0/0), d=172.31.55.4  
(Serial0/1), len 28, policy route
```

Exercise Verification

You have completed this exercise when you attain this result:

- You achieve control of traffic that is sourced from the loopback interfaces of the internal router through PBR, while maintaining reachability to the core router.

Lab Exercise 7-1: Configuring EBGP for Two Neighbors

Complete this lab exercise to practice what you learned in the related lesson.

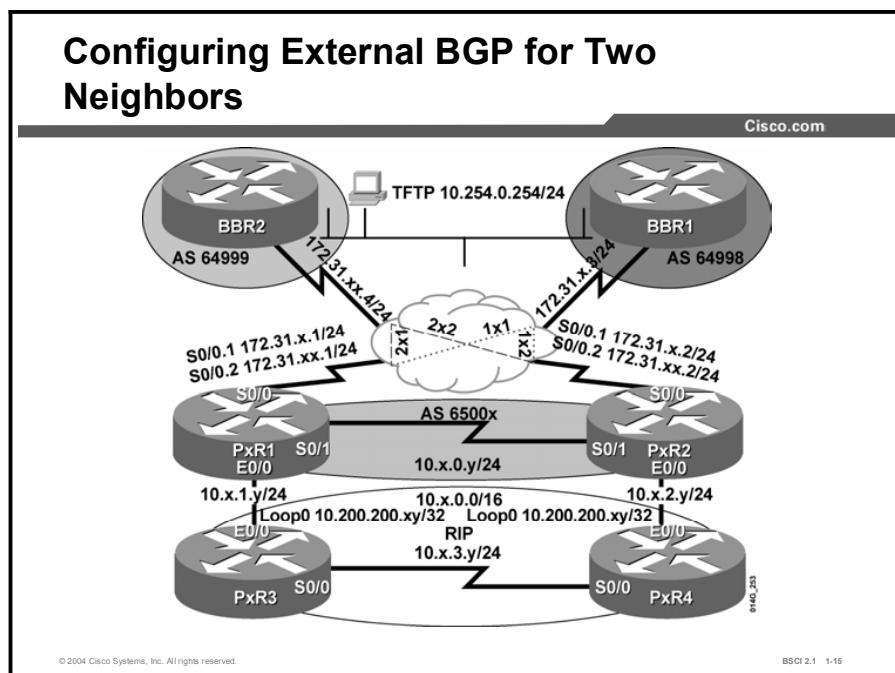
Exercise Objective

In this exercise, you will investigate how BGP works. After completing this exercise, you will be able to meet this objective:

- Configure a simple IBGP and EBGP network

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 1 [BBR1] and Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core (BBR1 and BBR2) through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router) #neighbor 10.x.0.2 remote-as 65003	Identifies a BGP neighbor.
(config-router) #network 10.x.1.0 mask 255.255.255.0	Advertises a network.
(config-router) #passive- interface s0/1	Configures a routing protocol not to send updates or hellos out the specified interface.
(config) #router bgp 65003	Enters into BGP router configuration mode; this router is in AS 65003.
#show ip bgp summary	Shows a summary of BGP neighbor status and activities.

Job Aids

There are no job aids for this lab exercise.

Task 1: Cleaning Up

In this task, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

Exercise Procedure

Complete these steps:

- Step 1** Remove all OSPF configurations from the edge routers, but leave RIPv2 enabled.
- Step 2** At the edge routers, disable IP PBR on the e0/0 interface. Additionally, remove any route maps and access lists that were configured in the previous labs.
- Step 3** At the edge routers, shut interface s0/0 and remove all configuration commands by using the **default interface s0/0** global configuration command.
- Step 4** At the edge routers, enable Frame Relay encapsulation on the s0/0 interface and then disable Frame Relay Inverse Address Resolution Protocol (ARP) on the s0/0 interface.
- Step 5** You will connect to both core routers (BBR1 and BBR2) in this lab, so you will need to create two multipoint subinterfaces on the serial 0/0 interface of each edge router.

Give subinterface S0/0.1 an IP address of 172.31.x.y/24 (where x is your pod number and y is your router number) and a Frame Relay map statement pointing to the BBR1 address of 172.31.x.3.

Give the second subinterface, S0/0.2, an IP address of 172.31.xx.y/24 and a Frame Relay map statement pointing to the BBR2 address of 172.31.xx.4.

Test each subinterface by pinging the BBR1 and BBR2 routers from both edge routers.

Your edge router S0/0 configuration should resemble the following:

```
P3R1(config-if)#int s0/0.1 multipoint
P3R1(config-subif)#ip address 172.31.3.1 255.255.255.0
P3R1(config-subif)#frame-relay map ip 172.31.3.3 131 broadcast
P3R1(config-subif)#int s0/0.2 multipoint
P3R1(config-subif)#ip address 172.31.33.1 255.255.255.0
P3R1(config-subif)#frame-relay map ip 172.31.33.4 231
broadcast
```

Task 2: Configuring BGP

In this task, you will configure basic BGP on the edge routers.

Exercise Procedure

Complete these steps:

- Step 1** Configure BGP on the edge routers in the pod (PxR1 and PxR2), using AS 6500 x , where x is your pod number.

Note Only the edge routers will run BGP in this lab. The internal routers will continue using RIPv2.

Configure PxR1 and PxR2 with two EBGP neighbors, the BBR1 (AS 64998) and BBR2 (AS 64999), and as IBGP neighbors to each other. BBR1 has the IP address of 172.31.x.3, and BBR2 is 172.31.xx.4. Use the 10.x.0.y address for establishing the IBGP session between the two edge routers.

- Step 2** Configure the edge routers to advertise your pod 10.x.0.0/24, 10.x.1.0/24, 10.x.2.0/24 and 10.x.3.0/24 networks to the core. There are two points to remember:
- a) The 10.0.0.0 network is subnetted, so you will need to use the **mask** option in the **network** command to announce the subnets.
 - b) The networks listed in the network statement must match the networks in the routing table exactly.
- Step 3** At the edge routers, verify that all three BGP neighbor relationships are established, using the **show ip bgp summary** command.

Do you see one IBGP neighbor and two EBGP neighbors?

How many prefixes have been learned from each BGP neighbor?

```
P3R1#show ip bgp summary
BGP router identifier 10.200.200.31, local AS number 65003
BGP table version is 25, main routing table version 25
17 network entries and 50 paths using 3449 bytes of memory
15 BGP path attribute entries using 900 bytes of memory
8 BGP AS-PATH entries using 192 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 17/15 prefixes, 51/1 paths, scan interval 15 secs
Neighbor          V   AS MsgRcvd MsgSent    TblVer  InQ OutQ
Up/Down  State/PfxRcd
10.3.0.2        4 65003      11      10      25      0      0
00:01:19          16
172.31.3.3       4 64998      10      11      25      0      0
00:01:57          17
172.31.33.4      4 64999      11       7      25      0      0
00:02:00          17
```

- Step 4** At the edge routers, display the BGP routing information base using the **show ip bgp** command. Verify that you have received routes from the core and from the other edge router. Look at the IP routing table on the edge routers. Are the BGP routes present?
- Step 5** Telnet to the core routers, BBR1 (172.31.x.3) and BBR2 (172.31.xx.4). Look at the IP routing table. Are the BGP routes present for your pod? End the Telnet session.
- Step 6** At the edge routers, because the network statement for RIPv2 includes the entire 10.0.0.0 network, RIPv2 is running between PxR1 and PxR2. You do not want it to do that, because for this lab, you want to run only IBGP between PxR1 and PxR2.
- Configure interface serial 0/1 as a passive interface for RIPv2 on both edge routers, under the RIP router configuration mode.
- Step 7** At the edge routers, use the **show ip protocols** command to verify the passive interface configuration and the BGP routing protocol.

```
P5R1#show ip protocols
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 22 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Redistributing: rip
    Default version control: send version 2, receive version 2
        Interface          Send   Recv Triggered RIP  Key-chain
        Ethernet0/0         2       2
        Loopback0            2       2
    Automatic network summarization is not in effect
    Maximum path: 4
    Routing for Networks:
        10.0.0.0
    Passive Interface(s):
        Serial0/1
    Routing Information Sources:
    Routing Information Sources:
        10.5.0.2           120      00:01:14
        10.5.1.3           120      00:00:26
    Distance: (default is 120)
    Routing Protocol is "bgp 65005"
        Outgoing update filter list for all interfaces is not set
        Incoming update filter list for all interfaces is not set
        IGP synchronization is enabled
        Automatic route summarization is enabled
```

```

Neighbor(s) :
      Address          FiltIn FiltOut DistIn DistOut Weight
RouteMap

      10.5.0.2
      172.31.5.3
      172.31.55.4

Maximum path: 1

Routing for Networks:
Routing Information Sources:
      Gateway        Distance   Last Update
      10.5.0.2        200       00:10:51
      172.31.55.4     20        00:10:35
      172.31.5.3      20        00:24:35

Distance: external 20 internal 200 local 200

```

- Step 8** You are not redistributing BGP into RIPv2, so the internal routers will not know any routes outside your pod. In a previous lab, you configured RIPv2 to pass a default route to the internal pod routers, PxR3 and PxR4, using the **default-information originate** command under the RIP router configuration.

Verify that the default route is still present.

- Step 9** Verify connectivity by pinging the TFTP server (10.254.0.254) from the edge routers. If this works, then ping the TFTP server from the internal routers.

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have successfully configured IBGP on R1 and R2, and EBGP between R1, R2, BBR1, and BBR2.
- You can ping the TFTP server from all pod routers.

Lab Exercise 7-2: Configuring Fully Meshed IBGP

Complete this lab exercise to practice what you learned in the related lesson.

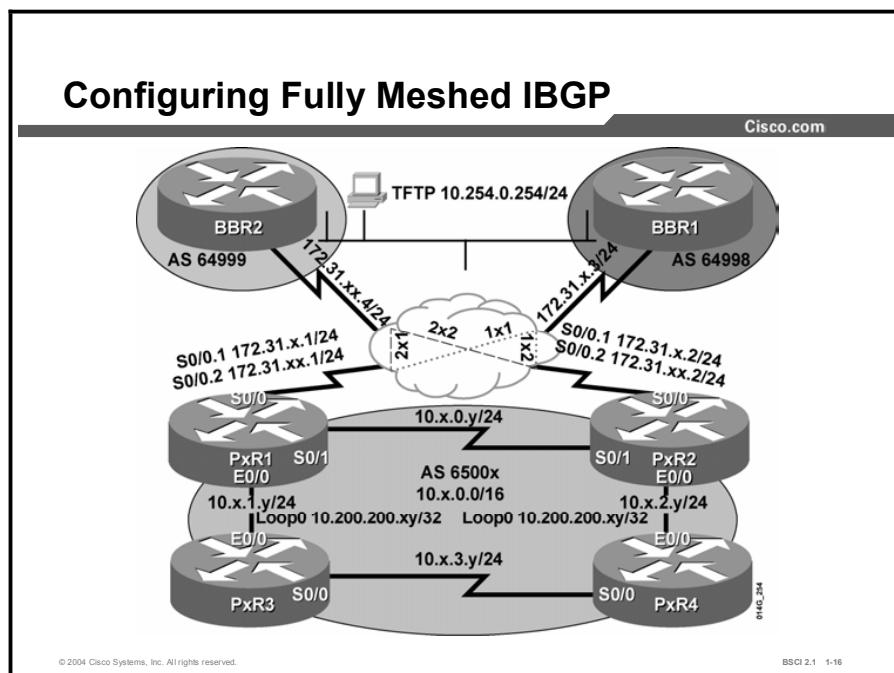
Exercise Objective

In this exercise, you will investigate how BGP runs inside an AS. After completing this exercise, you will be able to meet this objective:

- Configure full-mesh IBGP

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 1 [BBR1] and Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core (BBR1 and BBR2) through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router) #neighbor 10.200.200.xy next-hop-self	Advertises the next hop to this neighbor.
(config-router) #neighbor 10.200.200.xy update-source lo0	Peers with a neighbor using a loopback.
(config-router) #no synchronization	Turns off the synchronization rule.
#show ip bgp	Shows the BGP routing table.

Job Aids

There are no job aids for this lab exercise.

Task 1: Configuring Fully Meshed IBGP

In this task, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

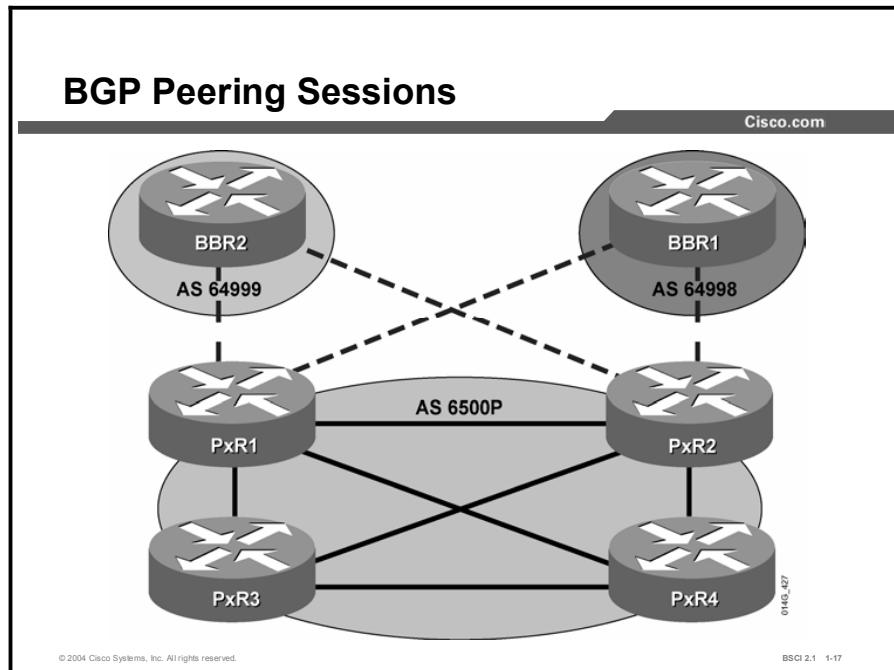
Exercise Procedure

Complete these steps:

- Step 1** Configure full-mesh IBGP between the PxR1, PxR2, PxR3, and PxR4 routers. Use the loopback address 10.200.200.xy to establish the IBGP session between the edge routers and the internal routers, and the IBGP session between the internal routers.

Recall that RIP is advertising this network, so the routers can be configured to use that loopback IP address of the network to establish an IBGP session.

-
- Note** There should be six IBGP sessions total, including one of the IBGP sessions between the two edge routers that were configured in the last lab. The figure here illustrates the BGP peering sessions. The dotted lines indicate EBGP peers, and the solid lines indicate IBGP peers.
-



- Step 2** Configure each internal router to advertise to its loopback interface 10.200.200.xy/32 in BGP.

- Step 3** Verify that the appropriate BGP neighbor relationships have been established.

Each edge router should see two EBGP neighbors and three IBGP neighbors. Each internal router should see three IBGP neighbors.

Your display for the edge router should resemble the following:

```
P3R2#sh ip bgp summary
BGP router identifier 10.200.200.32, local AS number 65003
BGP table version is 29, main routing table version 29
21 network entries and 38 paths using 3405 bytes of memory
13 BGP path attribute entries using 780 bytes of memory
7 BGP AS-PATH entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 22/1 prefixes, 39/1 paths, scan interval 15 secs
Neighbor          V     AS MsgRcvd MsgSent   TblVer InQ OutQ
Up/Down State/PfxRcd
10.3.0.1          4 65003    497      493       29     0     0
08:03:43          21
10.200.200.34    4 65003      4        9       29     0     0
00:00:14          1
10.200.200.33    4 65003      4        9       29     0     0
00:00:14          1
172.31.3.3        4 64998    501      497       29     0     0
08:03:45          17
172.31.33.4      4 64999      0        0       0     0     0
07:00:23          17
```

- Step 4** Use the **show ip bgp** command on the internal routers to determine the next hop for the route to the 10.254.0.0/24 network in the core.

What are the next-hop IP addresses for the routes to the 10.254.0.0/24 network in the core?

Which path is selected as the best path to the 10.254.0.0/24 network?

- Step 5** Display the IP routing table of the edge routers.

Is there a route to the 10.254.0.0/24 network?

Display the IP routing table of the internal routers. Is there a route to the 10.254.0.0/24 network? Why or why not?

The internal routers do not know how to reach the next-hop address, so they do not install the routes in their routing table if the next hop is not reachable. You can either advertise the next-hop network via an IBGP, or tell the edge routers to advertise themselves as the next hop. You will choose the second alternative.

- Step 6** Use the **next-hop-self** command to change the next hop that is advertised into the pod on the edge routers (PxR1 and PxR2).

Step 7 On the internal routers, PxR3 and PxR4, use the **show ip bgp** command once more to see the BGP route to 10.254.0.0/24.

What are the next-hop IP addresses for the routes to the 10.254.0.0/24 network now?

Have the internal routers installed these BGP routes in their routing table?

Why or why not?

The BGP synchronization rule is stopping BGP from installing the routes in the routing table.

What is the BGP synchronization rule?

Step 8 Because we are running full-mesh IBGP in our AS, we can safely turn off BGP synchronization on all the pod routers.

After turning off synchronization, look again at the routing table on the internal routers. You should see the BGP route to 10.254.0.0/24 now.

Step 9 From the internal routers, ping the TFTP server (10.254.0.254) to test connectivity.

Step 10 Determine what is the path that each interior router is using to reach the TFTP server.

Exercise Verification

You have successfully completed this exercise when you attain this result:

- You have configured full-mesh IBGP within your pod, and your routing tables contain BGP routes to the networks that are advertised by the core.

Lab Exercise 7-3: Configuring BGP Route Summarization and Examining the BGP Path Selection Process

Complete this lab exercise to practice what you learned in the related lesson.

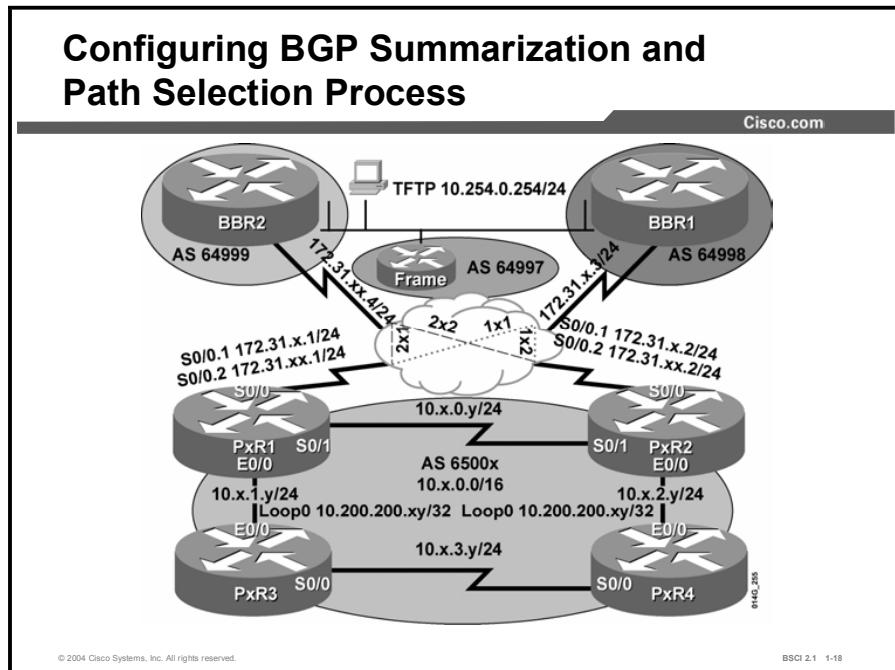
Exercise Objective

In this exercise, you will optimize BGP using route aggregation and investigate the BGP path selection process. After completing this exercise, you will be able to meet these objectives:

- Configure address summarization in BGP
- Determine the path selection process in use by BGP

Visual Objective

The figure illustrates what you will accomplish in this exercise.



Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (Backbone Router 1 [BBR1] and Backbone Router 2 [BBR2]) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
(config-router) #aggregate-address 10.x.0.0 255.255.0.0 summary-only	Advertises a summary route and suppresses all the more specific routes.

Job Aids

There are no job aids for this lab exercise.

Task 1: Configuring BGP Summarization and Path Selection Process

In this task, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

Exercise Procedure

Complete these steps:

Step 1 On edge routers PxR1 and PxR2, summarize your pod network to 10.x.0.0/16 to the core autonomous systems with the **aggregate address** command and **summary-only** option. You do not need to include the loopback interfaces on PxR3 and PxR4 in the summary.

Step 2 Telnet to either BBR1 or BBR2 and view the routing table. Is the aggregate address for your pod present?

From the BBR1 or BBR2 router, ping 10.x.3.3 and 10.xx.3.4 to test connectivity.

Step 3 On the edge routers, display the BGP table with the **show ip bgp** command.

Do you see your pod subnets being suppressed because of the **summary-only** option used with the **aggregate-address** command?

Examine the best path that is selected for network 10.97.97.0 in AS 64997 (AS 64997 is a new third router that is connected in the core.)

What is the next hop for this network?

Based on the BGP path selection process, why was this path chosen?

Your display should resemble the following:

```
P1R2#sh ip bgp
BGP table version is 42, local router ID is 10.1.2.2
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop        Metric LocPrf Weight
      Path
s> 10.1.0.0/24      0.0.0.0            0       32768 i
*> 10.1.0.0/16      0.0.0.0            0       32768 i
* i                 10.1.0.1           100      0 i
s> 10.1.1.0/24      10.1.2.4           2       32768 i
s> 10.1.2.0/24      0.0.0.0            0       32768 i
s> 10.1.3.0/24      10.1.2.4           1       32768 i
* 10.97.97.0/24    172.31.11.4          0
64999 64997 i
* i                 172.31.1.3          100      0
64998 64997 i
*>                  172.31.1.3          0
64998 64997 i
```

```
* i10.254.0.0/24      172.31.1.3          0    100    0
64998 i
*
*                  172.31.11.4          0
64999 64998 i
*>                 172.31.1.3          0    100    0
64998 I
```

Exercise Verification

You have successfully completed this exercise when you attain these results:

- You have summarized the pod network in BGP advertisements.
- You have determined the BGP path selection process that is used by your BGP routers.

Lab Exercise 7-4: BGP Path Manipulation Using the MED and Local Preference with Route Maps

Complete this lab exercise to practice what you learned in the related lesson.

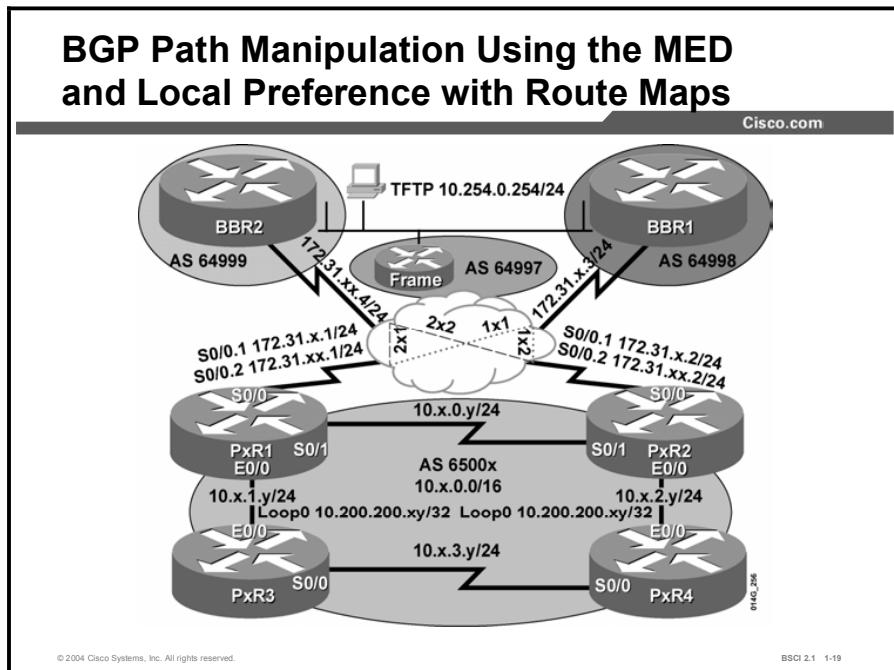
Exercise Objective

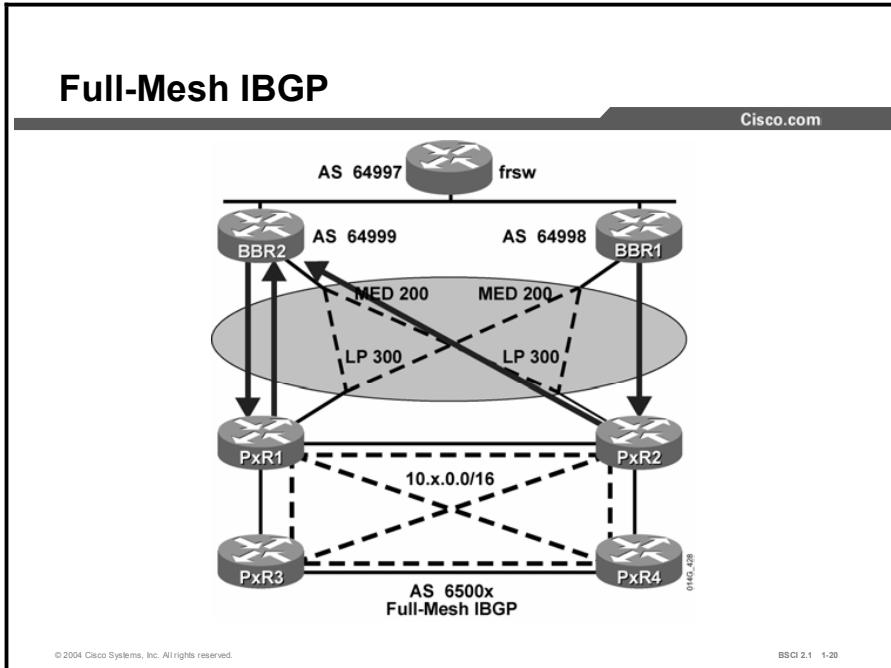
In this lab exercise, you will use a route map to change BGP MED and local preference values, thus affecting path selection. After completing this exercise, you will be able to meet these objectives:

- Configure a route map to change BGP local preference to influence outgoing traffic
 - Configure a route map to change the BGP MED to influence incoming traffic

Visual Objective

The figures illustrates what you will accomplish in this exercise.





Required Resources

In this configuration, a pod consists of four students, two laptops, and four routers (labeled PxR1 through PxR4) connected to a central core. These are the resources and equipment required to complete this exercise:

- Telnet or console access to pod routers
- Core (BBR1 and BBR2) configured for routing between pods

This lab exercise requires a topology of a pod and preconfigured core. No interaction between pods is required. A pod consists of these devices:

- Up to four end users
- Up to two end-user stations
- Four Cisco 2610 routers (or similar), labeled PxR1 through PxR4. PxR1 and PxR2 are edge routers. PxR3 and PxR4 are internal routers.

Each pod is connected to the core (BBR1 and BBR2) through the serial 0/0 port on PxR1 and PxR2.

Your instructor will provide the setup information that you need to complete this and subsequent lab exercises. Your instructor will assign you or your team to a pod and supply any required remote-access information. Complete the following information as provided by your instructor.

Table 1: Required Resources Information

Value	Information Provided by Your Instructor
Pod Number/Router Number	

Command List

The commands used in this exercise are described in the table here.

Table 2: Commands

Command	Description
<code>(config-route-map) #match ip address 3</code>	Used in a route map to match an IP address.
<code>(config-router) #neighbor 172.31.xx.4 route-map SET_PREF in</code>	Applies the route map to the incoming updates from a BGP neighbor.
<code>(config) #route-map SET_PREF permit 10</code>	Creates a route map named "SET_PREF".
<code>(config-route-map) #set local-preference 300</code>	Used in a route map to set the BGP local preference.
<code>(config-route-map) #set metric 200</code>	Used in a route map to set the BGP MED.

Job Aids

There are no job aids for this lab exercise.

Task 1: Using the MED and Local Preference with Route Maps for BGP Path Manipulation

To begin the lab exercises, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

Exercise Procedure

Complete these steps:

- Step 1** At the edge routers, look at the BGP table and notice the next hop for routes to the 172.31.x.0 and 172.31.xx.0 networks that connect the BBRx routers to the other pods.

Which path is the edge router using to reach the remote 172.31.x.0 networks? Why did BGP choose that path?

Which path is the edge router using to reach the remote 172.31.xx.0 networks? Why did BGP choose that path?

- Step 2** Your company has established a policy that all traffic exiting the AS, bound for any of the remote 172.31.x.0 and 172.31.xx.0 networks, should take the path through BBR2.

To comply with the above policy, configure the edge routers, PxR1 and PxR2, with a route map, setting local preference to 300 for any routes to the remote 172.31.x.0 and 172.31.xx.0 networks that are advertised by BBR2.

- Step 3** Look at the BGP table on the edge routers. Has the local preference changed?

- Step 4** When you configure a policy, it is not automatically applied to routes already in the BGP table. You can either reset the BGP relationship with BBR2, or configure the router to apply the policy to existing routes without resetting the relationship. This configuration is called a *soft* reconfiguration.

Use a soft reconfiguration to apply the policy to the routes that have come in from BBR2 with the command **clear ip bgp 172.31.xx.4 soft in**.

- Step 5** Take another look at the BGP table. Have the local preference values changed?

Which path is the edge router using to reach the remote 172.31.x.0 networks now?

Why did BGP choose that path even though the AS path is longer?

Which path is the edge router using to reach the remote 172.31.xx.0 networks now?

Why did BGP choose that path?

Your BGP table at the edge routers should look similar to the following:

```
p5r1#sh ip bgp
BGP table version is 85, local router ID is 10.200.200.51
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network Path	Next Hop	Metric	LocPrf	Weight
*> 172.31.1.0/24 64999 64998 i	172.31.55.4	300	0	
*	172.31.5.3	0	0	
64998 i				
* i 64999 64998 i	172.31.55.4	300	0	
*> 172.31.2.0/24 64999 64998 i	172.31.55.4	300	0	
*	172.31.5.3	0	0	
64998 i				
* i 64999 64998 i	172.31.55.4	300	0	
*> 172.31.3.0/24 64999 64998 i	172.31.55.4	300	0	
*	172.31.5.3	0	0	
64998 i				
* i 64999 64998 i	172.31.55.4	300	0	
*> 172.31.4.0/24 64999 64998 i	172.31.55.4	300	0	

*	172.31.5.3	0	0	
64998 i				
* i	172.31.55.4	300	0	
64999 64998 i				
*> 172.31.5.0/24	172.31.55.4	300	0	
64999 64998 i				
* i	172.31.5.3	0	0	
64998 i				
* i	172.31.55.4	300	0	
64999 64998 i				
Network Path	Next Hop	Metric	LocPrf	Weight
*> 172.31.6.0/24	172.31.55.4		300	0
64999 64998 i				
* i	172.31.5.3	0	0	
64998 i				
* i	172.31.55.4	300	0	
64999 64998 i				
*> 172.31.11.0/24	172.31.55.4	0	300	0
64999 i				
* i	172.31.5.3			0
64998 64999 i				
* i	172.31.55.4	0	300	0
64999 i				
*> 172.31.22.0/24	172.31.55.4	0	300	0
64999 i				
* i	172.31.5.3			0
64998 64999 i				
* i	172.31.55.4	0	300	0
64999 i				
*> 172.31.33.0/24	172.31.55.4	0	300	0
64999 i				
* i	172.31.5.3			0
64998 64999 i				
* i	172.31.55.4	0	300	0
64999 i				
*> 172.31.44.0/24	172.31.55.4	0	300	0
64999 i				
* i	172.31.5.3			0
64998 64999 i				
* i	172.31.55.4	0	300	0
64999 i				
*> 172.31.55.0/24	172.31.55.4	0	300	0
64999 i				
* i	172.31.5.3			0
64998 64999 i				
* i	172.31.55.4	0	300	0
64999 i				

```

* > 172.31.66.0/24  172.31.55.4          0   300   0
 64999 i

*
*           172.31.5.3          0
64998 64999 i

* i          172.31.55.4          0   300   0
64999 i

<output omitted>

```

- Step 6** Each of the core routers (BBR1 and BBR2) has multiple ways into your pod, for example, the direct path through your pod PxR1 or PxR2 router, or a path through the other core router, then to one of the pod edge routers.

Telnet to the core routers (BBR1 and BBR2) and examine the BGP tables.

Which path is the BBR1 router using to reach the 10.x.0.0 network of your pod?

Why did BGP choose that path?

Which path is the BBR2 router using to reach the 10.x.0.0 network of your pod?

Why did BGP choose that path?

- Step 7** Suppose your company has also established a policy for traffic inbound from the core. This policy states the following:

- Traffic from BBR1 to your pod 10.x.0.0 network should enter your pod through PxR1.
- Traffic from BBR2 to your pod 10.x.0.0 network should enter your pod through PxR2.

To accomplish the above policy, you want to do the following:

- Make the paths through PxR1 look unattractive to BBR2.
- Make the paths through PxR2 look unattractive to BBR1.

Right now, the MED for both paths is 0 in the BGP table of both BBR1 and BBR2, so BBR1 and BBR2 will pick the oldest EBGP path.

On PxR1, configure a route map setting a MED of 200 for routes to the internal network (10.x.0.0) of your pod and apply it to updates sent to BBR2.

- Step 8** On PxR2, configure a route map setting a MED of 200 for routes to the internal network (10.x.0.0) of your pod and apply it to updates sent to BBR1.

Remember that a lower MED is more attractive to BGP.

- Step 9** Perform a soft reconfiguration after you apply the policy to the BGP neighbor (BBR1 or BBR2) by using the **clear ip bgp ip-address soft out** command.

- Step 10** Telnet to the core routers and examine the BGP table. Verify that the MED changes have taken effect. Your output should look similar to the partial outputs that follow (using pod 5, as an example).

Notice that the path with the MED of 200 is not chosen as the best path.

What is the best path from BBR2 to your pod 10.x.0.0 network now?

What is the best path from BBR1 to your pod 10.x.0.0 network now?

```
BBR2#sh ip bgp
BGP table version is 417, local router ID is 172.31.66.4
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop            Metric LocPrf Weight
      Path
<output omitted>
*  10.5.0.0/16      172.31.55.1        200    0
65005 i
*
*          10.254.0.1
64998 65005 i
*>          172.31.55.2
65005 i
*
*          10.254.0.1
64997 64998 65005 i
*  10.97.97.0/24    10.254.0.3
64998 64997 i
*>          10.254.0.3
64997 i
<output omitted>
```

```
BBR1#sh ip bgp
BGP table version is 60, local router ID is 172.31.6.3
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop            Metric LocPrf Weight
      Path
<output omitted>

*  10.5.0.0/16      172.31.3.1        0
65003 64999 65005 i
*>          172.31.5.1
65005 i
*
*          10.254.0.2
64999 65005 i
```

```
*          172.31.5.2      200      0
65005 i
* 10.97.97.0/24  172.31.5.2      0
65005 64999 64997 i
*          172.31.5.1      0
65005 64999 64997
i*          10.254.0.3      0
64999 64997 I
<output omitted>
```

Exercise Verification

You have completed this exercise when you attain these results:

- You have changed the local preference of the specified routes.
- You have changed the MED of the specified routes.

Lab Exercise Answer Key

Lab Exercise 1-1: Basic Connectivity

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P3R2#show run
Building configuration...
Current configuration : 700 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R2
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
    ip address 10.3.2.2 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 172.31.3.2 255.255.255.0
    encapsulation frame-relay
    frame-relay map ip 172.31.3.3 132 broadcast
    no frame-relay inverse-arp
!
interface Serial0/1
    ip address 10.3.0.2 255.255.255.0
!
no ip classless
ip route 10.0.0.0 255.0.0.0 172.31.3.3
ip http server
ip pim bidir-enable
!
```

```

line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
end

```

Lab Exercise 1-2: NAT Using Access Lists and Route Maps

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R2#sh run
Building configuration...

Current configuration : 1183 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R2
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
  ip address 10.3.2.2 255.255.255.0
  ip nat inside
  half-duplex
!
interface Serial0/0
  ip address 172.31.3.2 255.255.255.0
  ip nat outside
  encapsulation frame-relay
  frame-relay map ip 172.31.3.3 132 broadcast

```

```

no frame-relay inverse-arp
!
interface Serial0/1
  ip address 10.3.0.2 255.255.255.0
  ip nat outside
!
  ip nat pool BBR 192.168.33.1 192.168.33.254 netmask
  255.255.255.0
  ip nat pool POD 10.3.0.96 10.3.0.127 netmask 255.255.255.0
  ip nat inside source route-map TO_BBR pool BBR
  ip nat inside source route-map TO_POD pool POD
  no ip classless
  ip route 10.0.0.0 255.0.0.0 172.31.3.3
  ip http server
  ip pim bidir-enable
!
access-list 100 permit ip 10.3.2.0 0.0.0.255 10.254.0.0
0.0.0.255
access-list 101 permit ip 10.3.2.0 0.0.0.255 any
route-map TO_BBR permit 10
  match ip address 100
!
route-map TO_POD permit 10
  match ip address 101
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
end

P3R4#sh run
Building configuration...

Current configuration : 453 bytes
!
version 12.2
service timestamps debug uptime

```

```

        service timestamps log uptime
        no service password-encryption
        !
        hostname P3R4
        !
        enable password cisco
        !
        ip subnet-zero
        !
        interface Ethernet0/0
            ip address 10.3.2.3 255.255.255.0
            half-duplex
        !
        interface Serial0/0
            ip address 10.3.3.4 255.255.255.0
        !
        interface Serial0/1
            no ip address
            shutdown
        !
        no ip classless
        ip route 0.0.0.0 0.0.0.0 10.3.2.2
        ip http server
        ip pim bidir-enable
        !
        line con 0
        line aux 0
        line vty 0 4
        !
    end

```

Lab Exercise 2-1: Migrating to a Classless Routing Protocol

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R2#sh run
Building configuration...
Current configuration : 849 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime

```

```
no service password-encryption
!
hostname P3R2
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
    ip address 10.3.2.2 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 172.31.3.2 255.255.255.0
    encapsulation frame-relay
    ip summary-address rip 10.3.0.0 255.255.0.0
    frame-relay map ip 172.31.3.3 132 broadcast
    no frame-relay inverse-arp
!
interface Serial0/1
    ip address 10.3.0.2 255.255.255.0
!
router rip
    version 2
    network 10.0.0.0
    network 172.31.0.0
    default-information originate
    no auto-summary
!
    ip classless
    ip route 0.0.0.0 0.0.0.0 172.31.3.3
    ip http server
    ip pim bidir-enable
!
line con 0
    exec-timeout 30 0
    logging synchronous
line aux 0
```

```

line vty 0 4
  no login
!
end

P3R4#sh run
Building configuration...
Current configuration : 640 bytes
!
version 12.2
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
!
hostname P3R4
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
  ip address 10.3.2.4 255.255.255.0
  half-duplex
!
interface Serial0/0
  ip address 10.3.3.4 255.255.255.0
  no fair-queue
!
interface Serial0/1
  no ip address
  shutdown
!
router rip
  version 2
  network 10.0.0.0
!
  ip classless
  ip http server

```

```

ip pim bidir-enable
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
end

```

Lab Exercise 3-1: Configuring and Tuning EIGRP

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R2#sh run
Building configuration...

Current configuration : 910 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R2
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
ip address 10.3.2.2 255.255.255.0
ip summary-address eigrp 1 0.0.0.0 0.0.0.0 5
half-duplex
!
interface Serial0/0
ip address 172.31.3.2 255.255.255.0
encapsulation frame-relay

```

```

ip summary-address eigrp 1 10.3.0.0 255.255.0.0 5
frame-relay map ip 172.31.3.3 132 broadcast
no frame-relay inverse-arp
!
interface Serial0/1
ip address 10.3.0.2 255.255.255.0
!
router eigrp 1
network 10.3.0.0 0.0.255.255

network 172.31.3.0 0.0.0.255
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
end

```

P3R2#

```

P3R4#sh run
Building configuration...

Current configuration : 686 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname P3R4
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Ethernet0/0
    ip address 10.3.2.4 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 10.3.3.4 255.255.255.0
    no fair-queue
!
interface Serial0/1
    no ip address
    shutdown
!
router eigrp 1
    network 10.3.0.0 0.0.255.255
    no auto-summary
    eigrp stub connected summary
    no eigrp log-neighbor-changes
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
    exec-timeout 30 0
    logging synchronous
line aux 0
line vty 0 4
    no login
!
end
```

Lab Exercise 4-1: Configuring and Examining OSPF in a Single Area

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
p1r2#sh run
Building configuration...

Current configuration : 783 bytes
!
version 12.1
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname p1r2
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!

interface Ethernet0/0
 ip address 10.1.2.2 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 172.31.1.2 255.255.255.0
 encapsulation frame-relay
 shutdown
 no fair-queue
 frame-relay map ip 172.31.1.3 112 broadcast
 no frame-relay inverse-arp
!
interface Serial0/1
 ip address 10.1.0.2 255.255.255.0
!
router ospf 1
 router-id 10.0.0.12
 log adjacency-changes
```

```

network 10.1.0.0 0.0.255.255 area 1
!
ip classless
ip http server
!
!
!
line con 0
exec-timeout 60 0
privilege level 15
logging synchronous
line aux 0
line vty 0 4
privilege level 15
no login
!
no scheduler allocate
end

p1r4#sh run
Building configuration...

Current configuration : 761 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname p1r4
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
ip address 10.200.200.14 255.255.255.255
!
interface Ethernet0/0

```

```
ip address 10.1.2.4 255.255.255.0
ip ospf priority 0
half-duplex
!
interface Serial0/0
ip address 10.1.3.4 255.255.255.0
no fair-queue
!
interface Serial0/1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.1.0.0 0.0.255.255 area 1
!
ip classless
ip http server
!
line con 0
exec-timeout 60 0
privilege level 15
logging synchronous
line aux 0
line vty 0 4
privilege level 15
no login
!
no scheduler allocate
end
```

Lab Exercise 4-2: Configuring OSPF for Multiple Areas and Frame Relay NBMA

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P1R2#sh run
Building configuration...
Current configuration : 912 bytes
!
version 12.1
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname P1R2
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
  ip address 10.1.2.2 255.255.255.0
  half-duplex
!
interface Serial0/0
  ip address 172.31.1.2 255.255.255.0
  encapsulation frame-relay
  ip ospf priority 0
  no fair-queue
  frame-relay map ip 172.31.1.3 112 broadcast
  no frame-relay inverse-arp
!
interface Serial0/1
  ip address 10.1.0.2 255.255.255.0
!
router ospf 1
  router-id 10.0.0.12
  log-adjacency-changes
  network 10.1.0.0 0.0.255.255 area 1
  network 172.31.1.0 0.0.0.255 area 0
!
ip classless
```

```

ip http server
!
line con 0
exec-timeout 60 0
privilege level 15
logging synchronous
line aux 0
line vty 0 4
privilege level 15
no login
!
no scheduler allocate
end

P1R4#sh run
Building configuration...
Current configuration : 741 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P1R4
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
ip address 10.200.200.14 255.255.255.255
!
interface Ethernet0/0
ip address 10.1.2.4 255.255.255.0
half-duplex
!
interface Serial0/0
ip address 10.1.3.4 255.255.255.0
no fair-queue
!
interface Serial0/1

```

```

no ip address
shutdown
!
router ospf 1
  log-adjacency-changes
  network 10.1.0.0 0.0.255.255 area 1
!
ip classless
ip http server
!
line con 0
  exec-timeout 60 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  privilege level 15
  no login
!
no scheduler allocate
end

```

Lab Exercise 4-3: Configuring OSPF for Multiple Areas and Frame Relay Point-to-Multipoint and Point-to-Point

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R2#sh run
Building configuration...
Current configuration : 1043 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R2
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup

```

```

!
interface Ethernet0/0
  ip address 10.3.2.2 255.255.255.0
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
  ip address 172.31.33.2 255.255.255.0
  ip ospf network point-to-multipoint
  frame-relay map ip 172.31.33.4 232 broadcast
!
interface Serial0/0.2 point-to-point
  ip address 10.33.0.2 255.255.255.0
  frame-relay interface-dlci 221
!
interface Serial0/1
  ip address 10.3.0.2 255.255.255.0
!
router ospf 1
  log-adjacency-changes
  network 10.3.0.0 0.0.255.255 area 3
  network 10.33.0.0 0.0.0.255 area 3
  network 172.31.3.0 0.0.0.255 area 0
  network 172.31.33.0 0.0.0.255 area 0
!
ip classless
ip http server
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
no scheduler allocate

```

```
end
```

Lab Exercise 4-4: Understanding the OSPF Database and Tuning OSPF

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P3R1#show run
Building configuration...

Current configuration : 1119 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
 ip address 10.3.1.1 255.255.255.0
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
 ip address 172.31.33.1 255.255.255.0
 ip ospf network point-to-multipoint
 frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/0.2 point-to-point
 ip address 10.33.0.1 255.255.255.0
 frame-relay interface-dlci 122
!
interface Serial0/1
```

```

ip address 10.3.0.1 255.255.255.0
clockrate 64000
!
router ospf 1
log-adjacency-changes
area 3 stub no-summary
area 3 range 10.3.0.0 255.255.0.0
network 10.3.0.0 0.0.255.255 area 3
network 10.33.0.0 0.0.0.255 area 3
network 172.31.3.0 0.0.0.255 area 0
network 172.31.33.0 0.0.0.255 area 0
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
no scheduler allocate
end

```

```

P3R3#show run
Building configuration...

Current configuration : 786 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R3
!
enable password cisco
!
ip subnet-zero

```

```
no ip domain-lookup
!
interface Loopback0
ip address 10.200.200.33 255.255.255.255
!
interface Ethernet0/0
ip address 10.3.1.3 255.255.255.0
ip ospf priority 0
!
interface Serial0/0
ip address 10.3.3.3 255.255.255.0
no fair-queue
clockrate 64000
!
interface Serial0/1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
area 3 stub
network 10.3.0.0 0.0.255.255 area 3
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
no scheduler allocate
end
```

Lab Exercise 4-5: Configuring OSPF Virtual Link (Optional)

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

P5R1:

```
Current configuration : 1146 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P5R1
!
enable password Cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
    ip address 10.5.1.1 255.255.255.0
!
interface Serial0/0
    no ip address
    encapsulation frame-relay
    no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
    ip address 172.31.55.1 255.255.255.0
    ip ospf network point-to-multipoint
    frame-relay map ip 172.31.55.4 251 broadcast
!
interface Serial0/0.2 point-to-point
    ip address 10.55.0.1 255.255.255.0
    frame-relay interface-dlci 122
!
interface Serial0/1
    ip address 10.5.0.1 255.255.255.0
    shutdown
    clockrate 64000
```

```

!
interface Serial0/2
  no ip address
  shutdown
!
interface Serial0/3
  no ip address
  shutdown
!
router ospf 1
  router-id 10.0.0.51
  log-adjacency-changes
  area 5 range 10.5.0.0 255.255.0.0
  area 5 virtual-link 10.200.200.53
  network 10.5.0.0 0.0.255.255 area 5
  network 10.55.0.0 0.0.0.255 area 5
  network 172.31.55.0 0.0.0.255 area 0
!
ip classless
ip http server
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
no scheduler allocate
end

```

```

P5R3:
Current configuration : 722 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname p5r3

```

```
!
enable password Cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
    ip address 10.200.200.53 255.255.255.255
!
interface Ethernet0/0
    ip address 10.5.1.3 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 10.5.3.3 255.255.255.0
    ip ospf network point-to-multipoint
    shutdown
    clockrate 64000
!
interface Serial0/1
    no ip address
!
router ospf 1
    log-adjacency-changes
    area 5 virtual-link 10.0.0.51
    network 10.5.0.0 0.0.255.255 area 5
    network 10.200.200.53 0.0.0.0 area 500
!
ip classless
ip http server
!
line con 0
line aux 0
line vty 0 4
    login
!
end
```

Lab Exercise 5-1: Configuring Integrated IS-IS in Multiple Areas

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P3R1#sh run
Building configuration...
Current configuration : 994 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0/0
    ip address 10.3.1.1 255.255.255.0
    ip router isis
    isis circuit-type level-1
!
interface Serial0/0
    no ip address
    encapsulation frame-relay
    shutdown
    no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
    ip address 172.31.33.1 255.255.255.0
    shutdown
    frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/0.2 point-to-point
    ip address 10.33.0.1 255.255.255.0
    shutdown
    frame-relay interface-dlci 122
!
```

```
interface Serial0/1
    ip address 10.3.0.1 255.255.255.0
    ip router isis
    clockrate 64000
    isis circuit-type level-2-only
!
router isis
    net 49.0031.1111.1111.1111.00
    summary-address 10.3.0.0 255.255.254.0
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
no scheduler allocate
end
!
P3R3#sh run
Building configuration...
Current configuration : 774 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R3
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
```

```
ip address 10.200.200.33 255.255.255.255
ip router isis
!
interface Ethernet0/0
ip address 10.3.1.3 255.255.255.0
ip router isis44
!
interface Serial0/0
ip address 10.3.3.3 255.255.255.0
ip router isis
no fair-queue
clockrate 64000
!
interface Serial0/1
no ip address
shutdown
!
router isis
net 49.0031.3333.3333.3333.00
is-type level-1
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
no scheduler allocate
end
```

Lab Exercise 6-1: Configuring Basic Redistribution

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P3R1#sh run
Building configuration...

Current configuration : 1258 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
!
no ip domain-lookup
!
interface Loopback0
    ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
    ip address 10.3.1.1 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 172.31.33.1 255.255.255.0
    encapsulation frame-relay
    ip ospf network point-to-multipoint
    frame-relay map ip 172.31.33.4 231 broadcast
    no frame-relay inverse-arp
!
interface Serial0/1
    ip address 10.3.0.1 255.255.255.0
!
router ospf 1
```

```

log-adjacency-changes
redistribute rip subnets
    network 172.31.0.0 0.0.255.255 area 0
    distribute-list 61 out rip
!
router rip
    version 2
    network 10.0.0.0
    default-information originate
    no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.31.33.4
ip http server
!
access-list 61 deny   10.200.200.0 0.0.0.255
access-list 61 permit any
!
line con 0
    exec-timeout 30 0
    logging synchronous
line aux 0
line vty 0 4
    no login
!
end

```

Lab Exercise 6-2: Tuning Basic Redistribution with Cisco IOS Tools

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R1#sh run
Building configuration...
Current configuration : 1510 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1

```

```

enable password cisco
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
  ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
  ip address 10.3.1.1 255.255.255.0
  half-duplex
!
interface Serial0/0
  ip address 172.31.33.1 255.255.255.0
  encapsulation frame-relay
  ip ospf network point-to-multipoint
  frame-relay map ip 172.31.33.4 231 broadcast
  no frame-relay inverse-arp
!
interface Serial0/1
  ip address 10.3.0.1 255.255.255.0
!
router ospf 1
  log-adjacency-changes
  redistribute rip subnets route-map CONVERT
  network 172.31.33.0 0.0.0.255 area 0
  distribute-list 61 out rip
!
router rip
  version 2
  network 10.0.0.0
  default-information originate
  no auto-summary
!
no ip classless
  ip route 0.0.0.0 0.0.0.0 173.31.33.4
  ip http server
!
access-list 61 deny 10.200.200.0 0.0.0.255
access-list 61 permit any
!
```

```

ip pim bidir-enable
!
route-map CONVERT permit 10
  match metric 1
  set metric 1000
!
route-map CONVERT permit 20
  match metric 2
  set metric 2000
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
end

```

Lab Exercise 6-3: Configuring Policy-Based Routing (Optional)

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R1#sh run
Building configuration...
Current configuration : 1757 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
  ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0

```

```

ip address 10.3.1.1 255.255.255.0
ip policy route-map PBR
!
interface Serial0/0
ip address 172.31.33.1 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
frame-relay map ip 172.31.33.4 231 broadcast
no frame-relay inverse-arp
!
interface Serial0/1
ip address 10.3.0.1 255.255.255.0
clockrate 64000
!
router ospf 1
log-adjacency-changes
redistribute rip subnets route-map CONVERT
network 172.31.33.0 0.0.0.255 area 0
!
router rip
version 2
network 10.0.0.0
default-information originate
no auto-summary
!
ip classless
ip http server
!
access-list 2 permit 10.200.200.0 0.0.0.255
route-map PBR permit 10
match ip address 2
set ip next-hop 10.3.0.2 (or set interface serial 0/1)
!
route-map CONVERT permit 10
match metric 1
set metric 1000
!
route-map CONVERT permit 20
match metric 2
set metric 2000

```

```

!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!
no scheduler allocate
end

```

Lab Exercise 7-1: Configuring EBGP for Two Neighbors

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R1#sh run
Building configuration...
Current configuration : 2182 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
  ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
  ip address 10.3.1.1 255.255.255.0
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  no frame-relay inverse-arp

```

```

!
interface Serial0/0.1 multipoint
  ip address 172.31.3.1 255.255.255.0
    frame-relay map ip 172.31.3.3 131 broadcast
!
!
interface Serial0/0.2 multipoint
  ip address 172.31.33.1 255.255.255.0
    frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/1
  ip address 10.3.0.1 255.255.255.0
  clockrate 64000
!
router rip
  version 2
  passive-interface Serial0/1
  network 10.0.0.0
  default-information originate

  no auto-summary
!
router bgp 65003
  bgp log-neighbor-changes
  network 10.3.0.0 mask 255.255.255.0
  network 10.3.1.0 mask 255.255.255.0
  network 10.3.2.0 mask 255.255.255.0
  network 10.3.3.0 mask 255.255.255.0
  neighbor 10.3.0.2 remote-as 65003
  neighbor 172.31.3.3 remote-as 64998
  neighbor 172.31.33.4 remote-as 64999
!
ip classless
ip http server
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4

```

```
    no login
!
no scheduler allocate
end
```

Lab Exercise 7-2: Configuring Fully Meshed IBGP

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```
P3R1#sh run
Building configuration...
Current configuration : 2328 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
  ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
  ip address 10.3.1.1 255.255.255.0
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
  ip address 172.31.3.1 255.255.255.0
  frame-relay map ip 172.31.3.3 131 broadcast
!
interface Serial0/0.2 multipoint
  ip address 172.31.33.1 255.255.255.0
```

```

frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/1
  ip address 10.3.0.1 255.255.255.0
  clockrate 64000
!
router rip
  version 2
  passive-interface Serial0/1
  network 10.0.0.0
  default-information originate
no auto-summary
!
router bgp 65003
  no synchronization
  bgp log-neighbor-changes
  network 10.3.0.0 mask 255.255.255.0
  network 10.3.1.0 mask 255.255.255.0
  network 10.3.2.0 mask 255.255.255.0
  network 10.3.3.0 mask 255.255.255.0
  neighbor 10.3.0.2 remote-as 65003
  neighbor 10.200.200.33 remote-as 65003
  neighbor 10.200.200.33 update-source Loopback0
  neighbor 10.200.200.33 next-hop-self
  neighbor 10.200.200.34 remote-as 65003
  neighbor 10.200.200.34 update-source Loopback0
  neighbor 10.200.200.34 next-hop-self
  neighbor 172.31.3.3 remote-as 64998
  neighbor 172.31.33.4 remote-as 64999
!
ip classless
ip http server
!
line con 0
  exec-timeout 30 0
  logging synchronous
line aux 0
line vty 0 4
  no login
!

```

```
no scheduler allocate
end

P1R3#sh run
Building configuration...
Current configuration : 948 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P1R3
!
no logging buffered
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0
 ip address 10.200.200.13 255.255.255.255
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
!
interface Serial0/0
 ip address 10.1.3.3 255.255.255.0
 clockrate 128000
!
interface Serial0/1
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
!
router bgp 65001
 no synchronization
```

```

bgp log-neighbor-changes
network 10.200.200.13 mask 255.255.255.255
neighbor 10.200.200.11 remote-as 65001
neighbor 10.200.200.11 update-source Loopback0
neighbor 10.200.200.12 remote-as 65001
neighbor 10.200.200.12 update-source Loopback0
neighbor 10.200.200.14 remote-as 65001
neighbor 10.200.200.14 update-source Loopback0
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
end

```

P1R3#

Lab Exercise 7-3: Configuring BGP Route Summarization and Examining the BGP Path Selection Process

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R1#sh run
Building configuration...
Current configuration : 2398 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
enable password cisco
ip subnet-zero
no ip domain-lookup
!

```

```

interface Loopback0
  ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
  ip address 10.3.1.1 255.255.255.0
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
  ip address 172.31.3.1 255.255.255.0
  frame-relay map ip 172.31.3.3 131 broadcast
!
interface Serial0/0.2 multipoint
  ip address 172.31.33.1 255.255.255.0
  frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/1
  ip address 10.3.0.1 255.255.255.0
  clockrate 64000
!
router rip
  version 2
  passive-interface Serial0/1
  network 10.0.0.0
  default-information originate
  no auto-summary
!
router bgp 65003
  no synchronization
  bgp log-neighbor-changes
  network 10.3.0.0 mask 255.255.255.0
  network 10.3.1.0 mask 255.255.255.0
  network 10.3.2.0 mask 255.255.255.0
  network 10.3.3.0 mask 255.255.255.0
  aggregate-address 10.3.0.0 255.255.0.0 summary-only
  neighbor 10.3.0.2 remote-as 65003
  neighbor 10.200.200.33 remote-as 65003

```

```

neighbor 10.200.200.33 update-source Loopback0
neighbor 10.200.200.33 next-hop-self
neighbor 10.200.200.34 remote-as 65003
neighbor 10.200.200.34 update-source Loopback0
neighbor 10.200.200.34 next-hop-self
neighbor 172.31.3.3 remote-as 64998
neighbor 172.31.33.4 remote-as 64999
!
ip classless
ip http server
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
no login
!
end

```

Lab Exercise 7-4: BGP Path Manipulation Using the MED and Local Preference with Route Maps

When you complete this lab exercise, your configuration will be similar to the following, with differences that are specific to your pod.

```

P3R1#sh run
Building configuration...
Current configuration : 2785 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname P3R1
!
enable password cisco
!
ip subnet-zero
no ip domain-lookup
!
interface Loopback0

```

```

ip address 10.200.200.31 255.255.255.255
!
interface Ethernet0/0
ip address 10.3.1.1 255.255.255.0
!
interface Serial0/0
no ip address
encapsulation frame-relay
no frame-relay inverse-arp
!
interface Serial0/0.1 multipoint
ip address 172.31.3.1 255.255.255.0
frame-relay map ip 172.31.3.3 131 broadcast
!
interface Serial0/0.2 multipoint
ip address 172.31.33.1 255.255.255.0
frame-relay map ip 172.31.33.4 231 broadcast
!
interface Serial0/1
ip address 10.3.0.1 255.255.255.0
clockrate 64000
!
router rip
version 2
passive-interface Serial0/1
network 10.0.0.0
default-information originate
no auto-summary
!
router bgp 65003
no synchronization
bgp log-neighbor-changes
network 10.3.0.0 mask 255.255.255.0
network 10.3.1.0 mask 255.255.255.0
network 10.3.2.0 mask 255.255.255.0
network 10.3.3.0 mask 255.255.255.0
aggregate-address 10.3.0.0 255.255.0.0 summary-only
neighbor 10.3.0.2 remote-as 65003
neighbor 10.200.200.33 remote-as 65003
neighbor 10.200.200.33 update-source Loopback0

```

```
neighbor 10.200.200.33 next-hop-self
neighbor 172.31.3.3 remote-as 64998
neighbor 172.31.33.4 remote-as 64999
neighbor 172.31.33.4 route-map SET_PREF in
neighbor 172.31.33.4 route-map SET_MED_HI out
!
ip classless
ip http server
!
access-list 3 permit 172.31.0.0 0.0.255.255
access-list 4 permit 10.3.0.0 0.0.255.255
route-map SET_MED_HI permit 10
  match ip address 4
  set metric 200
!
route-map SET_MED_HI permit 20
!
route-map SET_PREF permit 10
  match ip address 3
  set local-preference 300
!
route-map SET_PREF permit 20
!
line con 0
exec-timeout 30 0
logging synchronous
line aux 0
line vty 0 4
  no login
!
no scheduler allocate
end
```